FACULTAD DE INGENIERIA

ESCUELA ACADEMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

Sistema web para la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de Servicios Informáticos S.A.C – La Molina

TESIS PARA OBTENPER EL TITULO PROFESIONAL DE INGENIERIO DE SISTEMAS

AUTOR:

José Miguel Aguirre Ventura

ASESOR METODOLOGICO:

Dr.: Hilario Manuel Falcón

LÍNEA DE INVESTIGACIÓN:

Sistemas de información y comunicaciones

LIMA-PERÚ

2018

Acta de Aprobación de Tesis

UCV UNIVERSIDAD CÉSAR VALLEJO	ACTA DE APROBACIÓN DE LA TESIS	Código : F07-PP-PR-02.02 Versión : 09 Fecha : 23-03-2018 Página : 1 de 1

El Jurado encargado de evaluar la tesis presentada por don(a) **AGUITRRE VENTURA JOSE MIGUEL** cuyo título es: **"SISTEMA WEB PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ALINEADA A LA NORMA ISO/IEC 27001 EN LA EMPRESA DE SERVICIOS INFORMÁTICOS S.A.C – LA MOLINA"** Reunido en la fecha, escuchó la sustentación y la resolución de preguntas por el estudiante, otorgándole el calificativo de: **(13) (TRECE)**.

Lima, San Juan de Lurigancho, 19 de Diciembre del 2018

MG. RENEE RIVERA CRISÒSTOMO
PRESIDENTE

DR. HILARIO FALCON MANUEL
SECRETARIO

MG. MARÌA ACUÑA MELÈNDEZ
VOCAL

Elaboró	Dirección de Investigación	Revisó	Responsable del SGC	Aprobó	Vicerrectorado de Investigación

Dedicatoria

Dedico este esfuerzo personal y este logro académico y profesional:

A Dios por ser el principio y fin de todo cuanto existe y por ser el inspirador de mi vocación y el Desarrollo Humano.

A mi Abuela Mercedes Rufino, por haberme ayudado a estudiar años atrás, una carrera técnica, lo cual fue el resultado de todo esto.

A mi Papá Florencio por el apoyo, ánimo y ejemplo a seguir superándome en la vida.

A mi Madre Emma Ventura desde el cielo, por su apoyo permanente en todo proyecto que he iniciado en la vida.

A mis hermanos, familia y amigos con los que comparto todo lo que aprendo y de quienes también sigo aprendiendo.

A todos los beneficiarios de mi profesión, Ingeniería de Sistemas, a quienes espero aportar una mayor conciencia del valor y trascendencia de la condición humana.

Agradecimiento

Expreso mi agradecimiento:

En primer lugar, a mi Dios por darme la vida y cuidarme en los momentos más difíciles.

A mis maestros, por la enseñanza brindada durante mis estudios universitarios.

A mis compañeros con quienes compartí gratos momentos de intercambio de conocimientos y lazos de amistad

DECLARACIÓN DE AUTENTICIDAD

Yo JOSÈ MIGUEL AGUIRRE VENTURA, DNI N° 43061619, a efecto de cumplir con las disposiciones vigentes consideradas en el Reglamento de Grados y Títulos de la Universidad César Vallejo, Facultad de Ingeniería, Escuela de Ingeniería de Sistemas, declaro bajo juramento que toda la documentación que acompaño es veraz y auténtica.

Así mismo, declaro también bajo juramento que todos los datos e información que se presenta en la presente tesis son auténticos y veraces.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada por lo cual me someto a lo dispuesto en las normas académicas de la Universidad César Vallejo.

Lima, Diciembre 2018

.....

José Miguel Aguirre Ventura

Presentación

Señores miembros del jurado:
En cumplimiento de las reglas mencionadas en el Reglamento de Grados y Títulos de la Universidad César Vallejo presento ante ustedes la tesis titulada "SISTEMA WEB PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ALINEADA A LA NORMA ISO/IEC 27001 EN UNA EMPRESA DE SERVICIOS INFORMÁTICOS – LA MOLINA" la misma que someto a vuestra consideración y espero que cumpla con todos los requisitos de aprobación para obtener el título profesional de Ingeniero de Sistemas.

Esta investigación tiene como objetivo determinar el efecto de la implementación de un Sistema web para la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en una empresa de Servicios Informáticos – La Molina, la cual consta de siete capítulos; el capítulo I plantea una introducción describiendo la realidad problemática, trabajos previos, teorías relacionadas al tema, formulación del problema, justificación del estudio, hipótesis y los objetivos que lo guían, el capítulo II describe y explica el diseño de investigación, las variables de estudio y su operacionalización. Adicionalmente explica la población, la muestra y se detalla las técnicas e instrumentos para la recogida y procesamiento de la información, la validación y confiabilidad del instrumento, los métodos de análisis de los datos y aspectos éticos de la investigación, el capítulo III se refiere a los resultados de la investigación así como a la comprobación de las hipótesis, en el capítulo IV se presenta y se discuten los resultados de la investigación, en el capítulo V se presentan las conclusiones, en el capítulo VI se presentan las recomendaciones, en el capítulo VII se detallan las referencias bibliográficas utilizadas y finalmente se completa con los anexos.

Esperamos señores miembros del jurado que la presente investigación se ajuste a los requerimientos establecidos y que este trabajo dé origen a posteriores estudios.

El autor

ÍNDICE DE CONTENIDO

ACTA DE APROBACION DE TESIS……ii
DEDICATORIA……iii
AGRADECIMIENTO……iv
DELCLARACIÒN DE AUTENTICIDAD……v
PRESENTACIÒN……..vi
RESUMEN……viii
ABSTRACT……ix

I. INTRODUCCIÓN..... 10
1.1 Realidad Problemática.....11
1.2. Trabajos previos.....13
1.3 Teorías relacionadas al tema 30
1.4. Formulación del problema 51
1.5 Justificación del estudio.....51
1.6 Hipótesis 53
1.7. Objetivos.....54

I. MÉTODO 55
2.1. Diseño de investigación 56
2.2. Variable, operacionalización 58
2.3 Población y muestra 61
2.5 Técnicas e instrumentos de recolección de datos, validez y confiabilidad 62
2.6 Métodos de análisis de datos.....63
2.7 Aspectos éticos 64

III. RESULTADOS 65
3.1 Análisis Descriptivo 66
3.2 Análisis inferencial.....69

IV. DISCUSIÓN..... 85

V. CONCLUSIONES 88

VI. RECOMENDACIONES 90

VII. REFERENCIAS..... 92

ANEXOS 100

RESUMEN

La investigación realizada en el presente trabajo ha tenido el objetivo de estudiar el efecto de la implementación de un Sistema Web para la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en una empresa de Servicios Informáticos – La Molina.

La investigación realizada fue de tipo aplicada, con un diseño experimental de tipo pre experimental. La población estuvo conformada por 30 reportes diarios de reportes de Backup con información diaria del respaldo que se realiza a gran cantidad de servidores durante el periodo de un mes. Se usó como técnica de recopilación de datos la observación y se utilizó como instrumento la ficha de registro.

Los resultados de esta investigación confirman que la implementación del sistema web tuvo un efecto positivo para la gestión de la seguridad de la información; en cuanto a los indicadores de Porcentaje de Reportes entregados a Tiempo y Porcentaje de Reportes Íntegros generados.

Palabras Clave: Sistema Web, Gestión de la seguridad de la Información, Indicadores de porcentaje.

ABSTRACT

The objective of this research was to determine the effect of the implementation of a Web System for the management of information security aligned with ISO / IEC 27001 in a computer services company - La Molina.

The research carried out was of an applied type, with an experimental design of a pre experimental type. The population consisted of 30 daily reports of Backup reports with daily backup information that is made to a large number of servers during the period of one month. Observation was used as a technique for data collection and the registration form was used as an instrument.

The results of this research confirm that the implementation of the web system had a positive effect for the management of information security; as for the indicators of Percentage of Reports delivered to Time and Percentage of Integrated Reports generated.

Keywords: Web System, Information Security Management, Percentage Indicators

I. INTRODUCCIÓN

1.1 Realidad Problemática

A nivel internacional en nuestra actualidad, diversas empresas realizan inversiones económicas en Sistemas y Tecnologías de información con el fin de compensar las necesidades de la empresa y lograr un aumento del control sobre sus operaciones realizadas diariamente. Teniendo en cuenta un enfoque estratégico, los sistemas de información conforman un conjunto de elementos que aportan valor para obtener, procesar y mostrar la información para la alta gerencia quien puede usarla para una acertada toma de decisiones, el desempeño de la organización y, en última instancia, aumentar la rentabilidad del negocio (Laudon, 2012, p.12).

Con el paso de los años la información ha adquirido una importancia significativa para las empresas, por esto, la gestión de la seguridad de la información es tomada en cuenta dentro de los objetivos de las empresas y, por el contrario, y a pesar de esa reflexión conjunta, existen diversas empresas que huyen al cambio en lugar de estudiar la viabilidad de su aplicación (Aguirre y Aristizabal, 2013, p.15).

A nivel global, un 22% de las organizaciones analizadas habían sido víctimas de ataques a su seguridad y el 21% enfrentaba problemas con dispositivos, es decir, de cada cuatro empresas una sufre problemas de seguridad de información. Incluso en Latinoamérica, se halló que de cada diez empresas tres, experimentó una brecha de seguridad y el 16% ha enfrentado problemas de seguridad en dispositivos móviles (ISACA, 2012, p.30)

Investigaciones en Latinoamérica como las de Tabango y Guerrero (2014, p.24), indican que hoy en día ninguna organización está exenta de esta clase de vulnerabilidades, amenazas o ataques, que deben ser detectados a tiempo para así diseñar una serie de controles que las contrarresten, para lograrlo se han creado diferentes normas, entre las cuales existe la norma ISO/IEC 27001 que proporciona un marco de gestión de la seguridad de la información que puede adaptarse por cualquier organización pública o privada, grande o pequeña, que sin embargo, muchas empresas no ponen en práctica, poniendo en riesgo uno de los activos más importantes de la institución, la información.

A nivel nacional las entidades públicas y privadas diariamente producen información, informes, material, memorias y datos de diversos temas de mucha importancia para estas. Esto es la representación de toda la data que se necesita para su correcto funcionamiento. Los datos en la totalidad de los escenarios son almacenados en diversos recipientes, pudiendo ser físicos o digitales, además, está disponible para los usuarios que requieran utilizarla en sus labores de oficina ya sea para armar reportes gerenciales o calcular el flujo de dinero en las ventas u otras actividades que realiza la empresa. Se ha vuelto más difícil que un personal no autorizado acceda a ésta debido a los diversos métodos existentes y nuevos para extraer información. La principal problemática actual de las organizaciones que desean incursionar en el ámbito financiero es la escasa previsión y la falta de seguridad respecto a los peligros con la que cuentan sus activos información; el resultado de no tener las medidas necesarias para aminorar estos peligros puede llevar a la organización a pérdidas no solo de información, sino también económica (Barrantes y Hugo, 2012, p.45).

Ciertamente resulta riesgosa para la empresa, debido a que gran parte de la información importante y fundamental para la realización de los procesos críticos del proceso informativo puede ser amenazada y vulnerada ocasionando la interrupción de estos procesos, de esta manera, conllevan a una pérdida no solo de información, sino también a pérdidas financieras (Pinto, 2017, p.27).

Estudios han evidenciado que la instalación de software web para administrar la seguridad de la data permite un mayor control, para muchos esto es considerado una expectativa muy exigente que permitirá cubrir cosas puntuales (Pinto, 2017, p.32).

La empresa de Servicios Informáticos, llega oficialmente al Perú en 1932. A fines de esta década, se empieza a vender la máquina de escribir. Desde ese momento, dicha empresa comienza a crecer de forma exponencial y en 1950 llega la primera computadora electrónica marcada uno de los más grandes avances en la tecnología. Hoy, con más de 85 años de trayectoria en el Perú, se ha transformado para satisfacer los requerimientos de sus usuarios consumidores y trabajar junto con ellos para reinventar sus negocios a través de las nuevas tecnologías del mercado. Como toda

empresa se evidencia ciertas falencias en cuanto a la gestión de seguridad de la información tanto de forma global como específica en la que se tiene a la gestión de seguridad interna en la cual se presentan ciertos problemas para salvaguardar documentación que es generada o recibida como puede ser reportes, resúmenes de reuniones, actividades del personal y la guía técnica que representa las operaciones de la empresa; en cuanto a la administración de la seguridad de la data externa, muchas veces la información que adquiere no está a disposición de los usuario que trabajan en una empresa; y en cuanto a la seguridad de datos corporativa, muchas veces la documentación que la organización produce no se le brinda de la manera adecuada al público; de continuar esta problemática pueden originarse riesgos y un inadecuado uso de la información con la que cuenta la empresa, asimismo esta información si no es resguardada puede generar que la empresa se encuentre muchas veces vulnerables y podrían llegar a personas ajenas a la empresa e incluso a los propios competidores quienes podrían emplear dicha información para su propio beneficio, partiendo de ello es importante contar con un sistema web para la seguridad, disponibilidad, integridad y confiabilidad de la data alineado al estándar ISO/IEC 27001 de manera que se haga más fácil la tarea de evaluación de riesgo, la verificación de los mismos y el nivel de importancia de los activos. (Barrantes y Hugo, 2012, p.51)

1.2. Trabajos previos

Para el caso de este estudio, se hallaron antecedentes estudiantiles que hacen mención a los siguientes:

1.2.1. A nivel internacional:

Guamán (2015, p.3) en su trabajo de investigación: "*Diseño un* software de administración para la seguridad de la data *para Instituciones Militares*". Para el objetivo de alcanzar el título de Doctorado en administración de telecomunicaciones en la Universidad Técnica Estatal, Quito, Ecuador. Objetivo: Implementar un software de administración para la seguridad de la data destinada Instituciones Militares, siguiendo las normas internacionales orientados al ámbito militar y novedosos avances tecnológicos de la comunicación con la misión de

aportar a la modernización de éstas. Metodología: Modalidad de estudios de proyecto desarrollado en un estudio de campo e investigación monográfica documental. Conclusiones: Se estableció la factibilidad económica, técnica y operativa para fijar el Proyecto de un software de administración para la seguridad de la data para las instituciones Militares, que contribuyó a que las validaciones cumplan con las especificaciones acordes a las Instituciones Militares y se fije que el proyecto sea puesto en ejecución beneficiándose de todos lo que la institución prevee. De este modo los usuarios se encuentren en un ámbito de seguridad y tengan reconocimientos de las responsabilidades de seguridad de la información.

Doria (2015, p.3) en su trabajo de investigación: "Elaboración un software de administración para la seguridad de la data a través del uso del estándar internacional *ISO | IEC 27001:2013"* en el área de informática y comunicaciones de la Universidad de Córboda, por la universidad estatal a distancia facultad de ingeniería e investigación especializada en resguardo de la información. Objetivo: Elaborar un software web de protección de la data a través de la implantación del estándar ISO IEC 27001:2013. Metodología: Tipo de investigación no experimental. Investigación cualitativa. Conclusiones: Por medio de la etapa de diseño se estableció los pilares para luego seguir con la implantación del software de administración de seguridad de la data tomando en cuenta las buenas prácticas de las normas de seguridad internacional, y empleando la metodología de estudio de amenazas se determinan que objetos son los más vulnerables y que necesiten más supervisión de seguridad para así fijar una estrategia para la garantizar que los servicios continúen funcionando con normalidad.

Aguirre y Aristizabal (2013, p.3) en su trabajo de investigación: "Elaboración un software de administración para la seguridad de la data *para la empresa La Ofrenda"*. Con deseos de alcanzar el grado en licenciado en ingeniería de sistemas y computación de la Universidad Tecnológica de Pereira; Pereira, Colombia. Objetivo Elaboración un software de administración para la seguridad de la data para la empresa La Ofrenda". Para la obtención del grado de licenciado en ingeniería informática. Metodología: Tipo aplicada y diseño cuasi

experimental. Conclusión: Por medio de la etapa de diseño se estableció los pilares para luego seguir con la implantación del software de administración de seguridad de la data tomando en cuenta las buenas prácticas de las normas de seguridad internacional, y empleando la metodología de estudio de amenazas se determinan que objetos son los más vulnerables y que necesiten más supervisión de seguridad para así fijar una estrategia para la garantizar que los servicios continúen funcionando con normalidad.

Suárez (2015, p.3) en su trabajo de investigación "Elaboración e instalación de un software de administración para la protección de la data *en la institución Suárez Padilla,* que ofrezca seguridad a la información de la empresa". Tesis para obtener el título de ingeniero informático de la Universidad Estatal a Distancia, Colombia. Objetivo: Elaboración e instalación de un software de administración para la seguridad de la data *en la institución Suárez Padilla,* que ofrezca seguridad a la información de la empresa, con el fin de aumentar la alta seguridad para la información y proteger los activos frente a ataques informáticos. Metodología: Para esta investigación se utilizó el modelo internacional de administración de riesgos basados en la ISO 27005 para el control de riesgos relacionados a la seguridad de la data. La implantación de un software de administración de la seguridad de la información aumento la confiabilidad entre los usuarios e incrementó la imagen de la empresa frente a sus competidores.

Guzmán y Taborda, (2015, p.3) en su trabajo de investigación "Elaboración un software de administración para la seguridad informática para organizaciones del rubro textil en las ciudades de Colombia mediante la auditoria.". Tesis para lograr el título de ingeniero para seguridad en la información de la Universidad Estatal a Distancia, Colombia. Objetivo: Diseñar un SGSI en el aumento en seguridad de información, basados con procedimientos de auditoria, los cuales permitan hacer un diagnóstico de la situación actual que enfrentan las Pymes del sector textil en Medellín, Itagüí y Bogotá D.C. Metodología: La investigación fue de tipo aplicada. Conclusión: Durante la etapa de identificación, auditoria y lista de chequeo, se puede dimensionar herramientas de software, protocolos, procedimientos y actividades que mitiguen el riesgo en las empresas Color Shcp y

Guille Sport, implementando el desarrollo de respuestas de prevención y corrección, para cada uno de los controles marcados para garantizar en un porcentaje alto un óptimo funcionamiento de la organización con respecto a la seguridad informativa.

Carolina (2017, p.3) en su trabajo de investigación "Elaboración un software de administración para la seguridad informática *(SGSI) basados en la norma ISO/IEC 27001:2013*". Tesis de grado de la Institución Universitaria Politécnico Grancolombiano, Colombia. Objetivo: Elaboración un software de administración para la seguridad informática basados en la norma ISO/IEC 27001:2013. Metodología: La investigación es de tipo de cuantitativa y cualitativa. Conclusión: El estudio de riesgos que afectan a los activos informáticos intangibles en las diversas oficinas de la institución, sirvió para detectar el poco conocimiento del tema origina riesgos en los procedimientos que se efectúan con respecto a confidencialidad, integridad y disponibilidad.

Guzmán (2015, p.3) en su trabajo de investigación "*Elaboración un software de administración para la seguridad informática para una empresa del rubro financiero de segundo nivel"*. Tesis de grado de la Institución Universitaria Politécnico Grancolombiano, Colombia. Objetivo: Elaboración un software de administración para la seguridad informática para una empresa del rubro financiero de segundo nivel, siguiendo el estándar NTC-ISO-IEC 27001:2013. Metodología: La investigación presento un método de campo. Conclusión: De acuerdo al organigrama tecnológico y a las aptitudes de la oficina designada, la organización se ubica en un nivel Medio de estatus, que envuelve un esfuerzo destacable para la ejecución del software de administración para la seguridad informática, por ende, se ve reflejado en las diversas estrategias de operación que se crearon durante el proyecto que están dirigidos a dar acatamiento a los requisitos establecidos por el estándar ISO/IEC 27001:2013.

Molina (2015, p.3) en su trabajo de investigación "*Definición y validación de procesos de administración para la seguridad informática para la organización Amisoft"*. Trabajo de investigación para alcanzar el título en maestría de

tecnologías en la información de la Universidad de Chile, Chile. Objetivo: Conceptualizar y validar procesos relevantes para la gestión de seguridad de la información de la empresa Amisoft de acuerdo a la norma ISO/IEC 27001:2013. Metodología: La investigación fue de diseño pre experimental. Conclusión: Luego de las modificaciones realizadas, el AFP ha mejorado: la administración de riesgos, recursos humanos, manipulación de activos, controles para acceso. Del mismo modo, se ha notado un aumento en la respuesta a incidentes y la continuidad del negocio.

Berrio (2016, p.3) en su trabajo de investigación "*Metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad de información sobre la norma* ISO/IEC 27001*"*. Tesis para obtener el grado académico de maestría en ingeniería informática de la Universidad Estatal de Colombia, Colombia. Objetivo: Diseñar una metodología para la valoración del desempeño de los sistemas de gestión de seguridad de la información basado en la norma ISO/IEC 27001. Metodología: La investigación ha usado el método Delphi. Conclusión: La instalación de software de administración para la seguridad informática demanda seguir la evolución de las tecnológicas, en este sentido, el departamento de sistemas dispone de un rol muy importante, pues tiene que plantear instrumentos metodológicos para la prevención y para la identificación de amenazas relacionadas con el incremento de ataques informáticos, considerando que la mayoría de oficinas de una empresa están interconectadas.

Maureira (2017, p.3) en su trabajo de investigación "*Norma ISO/IEC 27001 aplicada a una carrera universitaria"*. Tesis dirigida a lograr un grado en ingeniero civil informático de la Universidad Andrés Bello, Chile. Objetivo: Aplicar la norma ISO27001 en la escuela universitaria de Ingeniería en Telecomunicaciones de la Universidad Andrés Bello, con la finalidad de proponer un diseño de SGSI para supervisar la correcta auditabilidad, disponibilidad, confidencialidad e integridad informática. Metodología: La investigación es de tipo aplicada. Conclusión: Los sistemas informáticos en general tienen un rol importante con respecto al brindado de servicios a otras instituciones, satisfacción

de los usuarios y clientes, alcance de las metas e inclusive lograr una diferencia competitiva. Por el contrario, el empleo de las herramientas tecnológicas lleva a posibles escenarios de ataques informáticos que muchas veces no son conocidos en su totalidad y debido a esto la gerencia no presupuesta dinero para elaborar un plan de protección, tampoco busca implementar diseños de seguridad informática.

Bermúdez y bailón (2015, p.3) en su trabajo de investigación "*Estudio de la seguridad de la información siguiendo el estándar ISO/IEC 27001 – orientado a una compañía de servicios del rubro finanzas"*. Tesis para alcanzar un grado de ingeniero de sistemas de la Universidad Politécnica Salesiana, Guayaquil, Ecuador. Objetivo: Estudiar las actividades críticas relacionadas con la confidencialidad de la data que maneja la empresa y también la integridad de los datos almacenados en el repositorio digital alojado en el data center de la empresa a través del estándar internacional ISO / IEC 27001. La investigación realizada en la empresa mostró que aplicando la norma internacional ISO/IEC 27001se redujo las amenazas a la información almacenada en los servidores de base de datos de la organización, además se notó un incremento en seguir las buenas prácticas para evitar posibles daños informáticos provocados por errores humanos no intencionados.

Tola (2015, p.3) en su trabajo de investigación "*Elaboración un software de administración para la seguridad informática para una institución de asesoría y auditoría, siguiendo el modelo ISO/IEC 27001";* Tesis para grado en Institución Universitaria Politécnico Guayaquil-Ecuador. Objetivo: Elaboración un software de administración para la seguridad informática para la empresa A&CGroup S.A del rubro financiero de segundo nivel, siguiendo el estándar NTC-ISO-IEC 27001:2013. Metodología: La investigación presento un método de campo. Conclusión: De acuerdo al organigrama tecnológico y a las aptitudes de la oficina designada, la organización se ubica en un nivel Medio de estatus, que envuelve un esfuerzo destacable para la ejecución del software de administración para la seguridad informática, por ende, se ve reflejado en las diversas estrategias de operación que se crearon durante el proyecto que están dirigidos a dar acatamiento a los requisitos establecidos por el estándar ISO/IEC 27001:2013

Morán (2016, p.3) en su trabajo de investigación "*Diseño de un software web para la gestión administrativa de los equipos camineros del Gad Municipal de Pedro Carbo",* tesis dirigida a obtener el grado profesional de ingeniero en sistemas computacionales de la Universidad de Guayaquil-Ecuador. Objetivo: Desarrollar una solución Web para el GAD Municipal de Pedro Carbo mediante la utilización de herramientas Open Source, que permitan realizar la correcta administración de la información de solicitudes ciudadanas y tareas asignadas para los Equipos Camineros Municipales, obteniendo así informes para el departamento de Obras Públicas. Metodología: Usó la metodología XP (eXtreme Programming). Conclusión: Se logró tener un sistema Web que facilitó la usabilidad para diferentes usuarios desde diferentes puntos de conexión y a través de distintos dispositivos móviles como tablets, Smartphone, entre otros.

Urrego y Soto (2015, p.3) en su trabajo de investigación "Sistema de información web para agilizar la actividad de radicación y registro de actividades en el área tecnológica para pequeñas empresas (SIPRA)"*;* tesis dirigida a obtener el grado profesional de tecnólogo en sistematización de datos de la Universidad Distrital Francisco José de Caldas, Colombia. Objetivo: Desarrollar una solución Web para el GAD Municipal de Pedro Carbo mediante la utilización de herramientas Open Source, que permitan realizar la correcta administración de la información de solicitudes ciudadanas y tareas asignadas para los Equipos Camineros Municipales, obteniendo así informes para el departamento de Obras Públicas. Metodología: Usó la metodología XP (eXtreme Programming). Conclusión: Los sistemas de información web presentan gran funcionalidad en el ámbito organizacional de cualquier empresa, porque ayuda a disminuir tiempos de procesamiento de la información.

Guerrón (2013, p.3), con su título: *"Elaboración un software de administración para la seguridad informática"*. Investigación final del Máster universitario en Seguridad informática y Telecomunicaciones de la Universidad Abierta de Cataluña, España. Objetivo: Aplicar la norma ISO27001 en la institución, con la finalidad de proponer un diseño de SGSI para supervisar la correcta auditoría,

disponibilidad, confidencialidad e integridad informática. Metodología: La investigación es de tipo aplicada. Conclusión: Los sistemas informáticos en general tienen un rol importante con respecto al brindado de servicios a otras instituciones, satisfacción de los usuarios y clientes, alcance de las metas e inclusive lograr una diferencia competitiva. Por el contrario, el empleo de las herramientas tecnológicas lleva a posibles escenarios de ataques informáticos que muchas veces no son conocidos en su totalidad y debido a esto la gerencia no presupuesta dinero para elaborar un plan de protección, tampoco busca implementar diseños de seguridad informática.

Salcedo (2014, p.3), con su título: *Plan de implementación del SGSI basado en la norma ISO 27001:2013*. Tesis de grado de la Universidad Abierta de Cataluña, España. Objetivo: Elaboración un software de administración para la seguridad informática. Metodología: Tipo aplicada y diseño cuasi experimental. Conclusión: Por medio de la etapa de diseño se estableció los pilares para luego seguir con la implantación del software de administración de seguridad de la data tomando en cuenta las buenas prácticas de las normas de seguridad internacional, y empleando la metodología de estudio de amenazas se determinan que objetos son los más vulnerables y que necesiten más supervisión de seguridad para así fijar una estrategia para la garantizar que los servicios continúen funcionando con normalidad.

Moyano y Suárez (2017, p.3), con su título: *Plan de implementación del SGSI basado en la norma ISO 27001:2013 para la empresa interfaces y soluciones*. Tesis de grado de la Universidad Francisco José de Caldas, Bogotá. Objetivo: Establecer un software de administración de la seguridad informática (SGSI) basado en la norma ISO 27001:2013 para los procesos del área de Tecnologías de la Información en la empresa Interfaces y Soluciones S.A.S. Conclusión: La Gestión de Riesgos realizada en la compañía estableció las bases para la mejora continua del SGSI. Por tanto, se identificaron y clasificaron los activos, se identificaron las amenazas, las vulnerabilidades y se estimaron los riesgos de acuerdo a criterios de confidencialidad, disponibilidad, integridad de la seguridad de la información y prioridades de la organización.

1.2.2. A nivel nacional:

Zeña (2015, p.3) en su tesis de estudio: "*Diseño de un software de administración para la seguridad informática para la Oficina principal de tecnología de la UNPRG*". Con la finalidad de obtener el título de Ingeniero de sistemas de la Universidad Nacional Pedro Ruiz Gallo; Lambayeque, Perú. Objetivo: Estudiar las actividades críticas relacionadas con la confidencialidad de la data que maneja la empresa y también la integridad de los datos almacenados en el repositorio digital alojado en el data center de la empresa a través del estándar internacional ISO / IEC 27001. Metodología: Enfoque cuantitativo y tipo descriptivo explicativo. Conclusión: La investigación realizada en la empresa mostró que aplicando la norma internacional ISO/IEC 27001se redujo las amenazas a la información almacenada en los servidores de base de datos de la organización, además se notó un incremento en seguir las buenas prácticas para evitar posibles daños informáticos provocados por errores humanos no intencionados.

Flores (2017, p.3) en su trabajo de investigación: "*Modelo de sistema en la administración en seguridad informática, en la Empresa SIAS SAC. – Chimbote; 2017*". Con motivo de lograr un grado profesional en Ingeniero de Sistemas de la Universidad Católica Los Ángeles de Chimbote; Chimbote, Perú.
Siguiendo las normas internacionales para la seguridad informática y empleando novedosos avances tecnológicos de telecomunicaciones con la misión de aportar a la modernización a la institución. Metodología: Modalidad de estudios de proyecto desarrollado en un estudio de campo e investigación documental. Conclusiones: Se estableció la factibilidad económica, técnica y operativa para fijar el Proyecto de un software de administración para la seguridad informática para la institución, lo que sirvió para validar que cumplan con las especificaciones acordes a las normas internacionales de seguridad informática y fijar que el proyecto se ejecute aprovechando todos los beneficios ofrecidos para la institución. De este modo los usuarios estarán en un ámbito de seguridad y se dará el reconocimiento de las responsabilidades relacionadas a la seguridad de la información.

Tarrillo y Correa (2015, p.3) en su trabajo de investigación: "*Diseño para un software de gestión de la seguridad informática basado en la norma internacional ISO/IEC 27001:2013 en la administración de la Municipalidad Distrital de Lambayeque setiembre 2013 - febrero 2014"*. Con el fin de obtener el grado profesional de ingeniero de sistemas de la Universidad Nacional Pedro Ruiz Gallo; Lambayeque, Perú. Objetivo: Diseño de un software en administración para la seguridad informática a través de una implantación del estándar ISO/IEC 27001:2013. Metodología: Tipo de investigación experimental. Investigación cuantitativa. Conclusiones: Por medio de la etapa de diseño se estableció los pilares informáticos para luego seguir con la implantación del software de administración de seguridad informática tomando en cuenta las buenas prácticas de las normas de seguridad internacional, y empleando la metodología de estudio de amenazas se determinan que objetos son los más vulnerables y que necesiten más supervisión de seguridad para así fijar una estrategia para la garantizar que los servicios continúen funcionando con normalidad.

Ochoa (2017, p.3) en su trabajo de investigación "*Software web de administración de seguridad informática guiada por un computador basada en la norma ISO 27001 en la Universidad Nacional José María Arguedas"*. Con deseos de lograr un grado de ingeniero de sistemas de la *Universidad Nacional José María Arguedas*. Objetivo Elaboración un software web de administración para la seguridad informática para la *Universidad Nacional José María Arguedas*". Metodología: Tipo aplicada y diseño experimental. Conclusión: Por medio de la etapa de diseño se estableció los pilares para luego seguir con la implantación del software de administración de seguridad informática tomando en cuenta las buenas prácticas de las normas de seguridad internacional, y empleando la metodología de estudio de amenazas se determinan que objetos son los más vulnerables y que necesiten más supervisión de seguridad para así fijar una estrategia para la garantizar que los servicios continúen funcionando con normalidad.

Suca (2014, p.3) en su trabajo de investigación “Elaboración e instalación de un software de administración para la seguridad informática *en entidades públicas del Estado*”. Tesis para obtener el título de ingeniero informático de la Universidad Católica de Santa María, Arequipa. Objetivo: Elaboración e instalación de un software de administración para la seguridad informática *en entidades públicas del Estado,* que ofrezca seguridad a la información de la institución, con el fin de aumentar la seguridad de la información y proteger los activos frente a ataques informáticos. Metodología: Para esta investigación se utilizó el estándar internacional de administración de riesgos basados en la ISO/IEC 27001:2008 en el control para riesgos relacionados a seguridad en la data. La implementaciòn de un software de administración de la seguridad informática aumento la confiabilidad entre los usuarios e incrementó la imagen de la institución.

Arisaca y Quispe (2016, p.3) en su trabajo de investigación *“Elaboración un software de administración para la seguridad informática, para la oficina funcional de informática del gobierno regional del Cusco*”. Tesis para obtener el grado de ingeniero en seguridad de la información de la Universidad Nacional de San Antonio ABAD del Cusco, Cusco. Objetivo: Diseño de un SGSI para aumentar seguridad en la información, basados con normas internacionales de auditoria que permitan hacer un diagnóstico de la situación actual de la institución. Metodología: La investigación es aplicada y con diseño experimental.

Ccesa (2017, p.3) en su trabajo de investigación *“Diseño de un software de administración de seguridad informática bajo la norma ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016”*. Tesis para optar el título de ingeniero informático de la Universidad Nacional de San Cristóbal de Huamanga, Ayacucho. Objetivo: Determinar las características del diseño de un software de administración de seguridad informática bajo la norma ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016. Metodología: La investigación es de tipo aplicada. Conclusión: Se determinó como características esenciales del diseño del SGSI para la Municipalidad Provincial de

Huamanga, el compromiso y apoyo de la alta dirección, el conocimiento de la organización, la adecuada identificación del alcance del SGSI, la evaluación de riesgos y la mejora continua.

Quispe y Vargas (2016, p.3) en su trabajo de investigación *"Desarrollo de un software web para aumentar el rendimiento administrativo de la Empresa Comercial Angelito de la Ciudad de Chepén"*. Tesis dirigida a obtener el título de ingeniero de sistemas de la Universidad Nacional de Trujillo, Trujillo. Objetivo: Diseñar de un sistema web para mejorar el control administrativo de la Empresa Comercial Angelito de la Ciudad de Chepén. Metodología: La metodología que empleo la investigación es de RUP (Rational Unified Process). Conclusión: El uso de un software web aumenta la rentabilidad en el área de ventas y de esta manera se consigue desarrollar una mejor atención a los clientes.

Cupitán (2017, p.3), con su título: "*Diseño de un software de administración para la seguridad informática para la empresa grupo Company S.A.C., Chimbote; 2015*". Con fin de obtener el grado de Ingeniero de sistemas para la Universidad Católica los Ángeles, Chimbote. Perú. Objetivo: Estudiar las actividades críticas relacionadas con la confidencialidad de la data que maneja la empresa y también la integridad de los datos almacenados en el repositorio digital alojado en el data center de la empresa a través del estándar internacional ISO / IEC 27001. Metodología: Enfoque cuantitativo y tipo descriptivo explicativo. Conclusión: La investigación realizada en la empresa mostró que aplicando la norma internacional ISO/IEC 27001se redujo las amenazas a la información almacenada en los servidores de base de datos de la organización, además se notó un incremento en seguir las buenas prácticas para evitar posibles daños informáticos provocados por errores humanos no intencionados.

Alcántara (2015, p.3), con su tesis: *"Manual de implantación de la seguridad según el estándar ISO/IEC 27001, para ayudar a la seguridad informática de la comisaria del norte P.N.P en la ciudad de Chiclayo"*. Tesis para optar el título de ingeniero de Sistemas y Computación de la Universidad Católica Santo Toribio de Mogrovejo, Chiclayo. Perú. Objetivo: Contribuir a mejorar el nivel de

seguridad de la Información, apoyado en la norma ISO/IEC 27001, en la institución Policial Comisaria del Norte – Chiclayo. Metodología: La investigación se caracterizó por ser aplicada. Conclusión: Con el manual de implantación, se consiguió aumentar el grado de seguridad informática en las aplicaciones de oficina de la institución policial. Esto evidenció un aumento de reglas de seguridad que fueron aplicadas y que contribuyeron que la institución logre incrementar el grado de seguridad informática.

1.2.3. A nivel regional

Espinoza (2013, p.3) en su trabajo de investigación: "*Elaboración de un software de administración de seguridad informática según la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo".* Con motivo de optar el grado de licenciado en Ciencias e Ingeniería de la Pontificia Universidad Católica del Perú; Lima, Perú. Objetivo: Elaborar un software de administración de seguridad informática según la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo. Metodología: Tipo experimental. Conclusión: el diseño de SGSI que ha sido presentado se adapta al objetivo actual de los procedimientos de producción, en donde se ha fundamentado los proyectos, y que este modelo podría tener variaciones ya que el objetivo estratégico y de gobierno de la entidad pueda tener cambios y de esta manera ciertas actividades del proyecto, también se verán reflejadas.

Justino (2015, p.3) en su trabajo de investigación "*Implementación de un software de administración de seguridad informática para una empresa inmobiliaria según el estándar ISO / IEC 27001:2013*". Con motivo de optar el grado de ingeniera informática de la Universidad Católica del Perú, Lima. Objetivo: Implementación de un software de administración de seguridad informática para una empresa inmobiliaria según el estándar ISO / IEC 27001:2013, ISO/IEC 27002:2013. Metodología: se basó en un diseño experimental. Conclusión: El estudio de riesgos que afectan a los activos informáticos intangibles en las diversas oficinas de la institución, sirvió para

detectar el poco conocimiento del tema origina riesgos en los procedimientos que se efectúan con respecto a confidencialidad, integridad y disponibilidad.

Ríos (2018, p.3) en su trabajo de investigación "*software web para aumentar el rendimiento en la administración de inventarios para la organizaciòn Comercial Lucerito*". Trabajo de investigación para lograr el grado de ingeniero de sistemas de información de la Universidad Norbert Wiener, Lima. Objetivo: Proponer un sistema web para mejorar el control de inventarios en la empresa Comercial Lucerito. Metodología: La investigación es de tipo proyectiva de método inductivo-deductivo. Conclusión: Se propuse un sistema web para mejorar el control de inventarios en la empresa Comercial Lucerito, debido a que esta no cuenta con un sistema que permita centralizar la información de sus diferentes puntos de ventas en un solo lugar, puesto que los registros de las entradas y salidas realizaban en cuadernos físicos, los cuales no estaban organizados.

Talavera (2015, p.3) en su trabajo de investigación "*Desarrollo de un software de administración de seguridad informática en la institución estatal de salud según norma ISO/IEC 27001:2013"*. Trabajo de investigación para optar el grado de ingeniero informático de la Pontificia Universidad Católica del Perú, Lima. Objetivo: Desarrollar un software de administración de seguridad informática para una institución estatal de salud según la norma ISO/IEC 27001:2013. Metodología: La investigación es de método inductivo-deductivo. Conclusión: Luego de la implementación del software de administración de seguridad informática se notó un aumento de las aptitudes del personal de la oficina de informática, que envuelve un esfuerzo destacable para la ejecución del software de administración para la seguridad informática, por ende, se ve reflejado en los diversas estrategias de operación que se crearon durante el proyecto que están dirigidos a dar acatamiento a los requisitos establecidos por el modelo ISO/IEC 27001:2013 y así garantizar un mejor servicio a los usuarios.

Santos (2016, p.3) en su trabajo de investigación "*Instalación, ejecución y mantenimiento de un software de administración de seguridad informática, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de*

software". Tesis dirigida a obtener el título de ingeniero informático de la Pontificia Universidad Católica del Perú, Lima. Objetivo: Instalación, ejecución y mantenimiento de un software de administración de seguridad informática, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software. Metodología: La investigación es de método inductivo-deductivo. Conclusión: La instalación, ejecución y mantenimiento de un software de administración de seguridad informática, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software garantiza la confidencialidad ya que se reduce los puntos vulnerables de la empresa en relación con el almacenamiento de la información.

Vilca (2017, p.3) en su trabajo de investigación "*Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa Geosurvey de la ciudad de Lima"*. Tesis para optar el grado de ingeniero de sistemas e informática de la Universidad de Huánuco. Objetivo: Determinar la mejora de implementar un sistema de gestión de seguridad de la información para la seguridad del área de recursos humanos de la empresa Geosurvey S.A. Metodología: La investigación presenta un enfoque cuantitativo y contó con un diseño pre experimental. Conclusión: La intervención en la empresa GEOSURVEY resultó en una mejora del sistema de gestión de seguridad de la información en su área de Recursos Humanos.

Vargas (2017, p.3) en su trabajo de investigación "*Sistema web para el proceso de venta en la empresa Calzatec E.I.R.L."*. Tesis para optar el grado de ingeniero de sistemas de la Universidad César Vallejo, Lima. Objetivo: Distinguir en efecto de un implementación Web en el proceso de ventas de la empresa CALZATEC E.I.R.L. Metodología: Esta investigación presenta es tipo aplicada – experimental. Conclusión: Como conclusión, un Software Web aumenta altamente el rendimiento para el proceso en ventas en la empresa CALZATEC E.I.R.L., pues ayudó a el incremento del Promedio de Pedidos por cliente, lo que facilitó lograr cumplir con las metas de esta investigación.

Fernández y Pacheco. (2014, p.3) en su trabajo de investigación "*Desarrollo de*

un software de administración de seguridad informática en la comandancia de operaciones guardacostas basada en la norma técnica peruana NTP-ISO/IEC 27001:2008". Tesis para optar el grado de ingeniero de computación y sistemas de la Universidad San Martín de Porras, Lima. Objetivo: Elaborar un sistema de gestión en seguridad informática en la comandancia de operaciones guardacostas basada en la norma técnica peruana NTP-ISO/IEC 27001:2008. Metodología: La investigación presentó el método planear, hacer, verificar y actuar usado por las normas NTP-ISO/IEC 27001:2008. Conclusión: El estudio de riesgos que afectan a los activos informáticos intangibles en las diversas oficinas de la institución, sirvió para detectar que el poco conocimiento del tema origina riesgos en los procedimientos que se efectúan con respecto a confidencialidad, integridad y disponibilidad.

Aguirre (2014, p.3) en su trabajo de investigación "*Desarrollo de un software de administración de seguridad informática en servicios postales del Perú S.A."*. Tesis para optar el grado de ingeniero informático de la Pontificia Universidad Católica del Perú, Lima. Objetivo: Desarrollar un software de administración de seguridad informática en servicios postales del Perú S.A con la norma NTP ISO/IEC 27001:2008 y la NTP-ISO/IEC 17999:2007. Metodología: La investigación fue de diseño pre experimental. Conclusión: Por medio de la etapa de diseño se estableció los pilares para luego seguir con la implantación del software de administración de seguridad informática tomando en cuenta las buenas prácticas de las normas de seguridad internacional, y empleando la metodología de estudio de amenazas se determinan que objetos son los más vulnerables y que necesiten más supervisión de seguridad para así fijar una estrategia para la garantizar que los servicios continúen funcionando con normalidad.

Espinoza (2013, p.3) en su trabajo de investigación "*Desarrollo de un software de administración de seguridad informática según el estándar ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo"*. Tesis para optar el grado de ingeniero informático de la Pontificia Universidad Católica del Perú, Lima. Objetivo: Desarrollar un software de

administración de seguridad informática según el estándar ISO/IEC 27001:2005 en una empresa de producción y comercialización de productos de consumo masivo. Metodología: La investigación utilizó como metodología base a Magerit II. Conclusión: El estudio de riesgos que afectan a los activos informáticos intangibles en las diversas oficinas de la institución, sirvió para detectar que el poco conocimiento del tema origina riesgos en los procedimientos que se efectúan con respecto a confidencialidad, integridad y disponibilidad.

Guillermo (2017, p.3) en su trabajo de investigación "*Implementación de un sistema Web para las ventas en la empresa One To One Contact Solutions"*. Tesis para optar el grado de ingeniero empresarial y de sistemas de la Universidad San Ignacio de Loyola, Lima. Objetivo: Implementar un Sistema Web, aplicando SCRUM y XP para mejorar el Proceso de Ventas en la Empresa One To One Contact Solutions. Metodología: La investigación es de tipo aplicada tecnológica, conto con un diseño pre experimental. Conclusión: El sistema web ha sido enfocado en hacer que el asesor de ventas esté conectado, es decir que no existan tiempos muertos, debido a que ahora se han aplicado modos de marcación, lo que se demuestra en los resultados donde el promedio de llamadas por cliente sea alrededor de 10 llamadas, aumentando la probabilidad de que se logre la contactabilidad y el posterior cierre de venta

Ramírez (2017, p.3) en su trabajo de investigación "*Implementación de un sistema web para mejorar el proceso de gestión académica en las escuelas de la PNP"*. Tesis para optar el título de licenciatura de ingeniero en computación y sistemas de la Universidad Peruanas de las Américas, Lima. Objetivo: Implementar el Sistema Web Académico para la mejora del proceso de Gestión Académica en las Escuelas de Formación de la PNP. Metodología: La investigación presenta un enfoque cuantitativo, conto con un diseño pre experimental. Conclusión: El Sistema web académico que se desarrolló mejora significativamente el proceso de Gestión Académica en las Escuelas de Formación de la PNP.

Callán, Ramos y Solano (2017, p.3) en su trabajo de investigación

"Implementación de un Sistema Web para el Control y Monitoreo de la Empresa AB Seguridad E.I.R.L.". Tesis para optar el título de ingeniero en computación y sistemas de la Universidad Peruanas de las Américas, Lima. Objetivo: Implementar un sistema web para el proceso de control y monitoreo de la empresa AB Seguridad E.I.R.L. Metodología: La investigación es de tipo aplicada. Conclusión: El implementar un sistema web facilita la obtención de conocimiento al cliente sobre los productos que brinda la Empresa. Es así como se mejora la calidad de la información sobre el uso de los extintores y la viabilidad de elección de productos dentro del stock de disponibilidad.

Aliaga (2013, p.3), con su título: *"Diseño de un sistema de administración de seguridad informática para un instituto educativo"*. Tesis para optar el título de Ingeniero Informático, que presenta el bachiller de la Pontificia Universidad Católica del Perú, Lima. Perú. Objetivo: El objetivo de este proyecto es diseñar un sistema de administración de seguridad informática para un instituto educativo según los estándares ISO/IEC 27001:2005 e ISO/IEC 27002:2005, apoyándose en el marco de negocios basados en COBIT. Metodología: Fue una investigación de tipo aplicada. Conclusión: Por medio de la etapa de diseño se estableció los pilares para luego seguir con la implantación del software de administración de seguridad informática tomando en cuenta las buenas prácticas de las normas de seguridad internacional, y empleando la metodología de estudio de amenazas se determinan que objetos son los más vulnerables y que necesiten más supervisión de seguridad para así fijar una estrategia para la garantizar que los servicios continúen funcionando con normalidad.

1.3 Teorías relacionadas al tema

1.3.1. Sistema web

1.3.1.1. Definición de sistema web

Para Berrospi y Pilar (2017, p.27) es considerada como una serie de diferentes partes o elementos que se hallan de manera organizada y relacionada entre sí, que tienden a interactuar de manera que se consigan las metas. El sistema recibe datos que tienden hacer la entrada, y a la misma provee la salida que sería la

información.

Así mismo, en la ingeniería informática se define aplicación web aquella herramienta en la cual un usuario puede utilizar a través de la conexión a un servidor web por medio de Internet o de una intranet a través de un navegador. Lo que significa que es una aplicación que se desarrolla en lenguajes sostenidos por el navegador web donde se lleva la ejecución. (Berrospi y Pilar, 2017, p.29).

Por su parte Baez (2012, p. 35) señala que un sistema web o llamado también aplicación web la cual está desarrollada e instalada no sobre una plataforma o un sistema operativo (Windows, Linux), los cuales están en servidores de internet o sobre una intranet (red local). Es casi igual a las páginas web que se acostumbra observar de manera frecuente, pero en sí el sistema web tiene una función muy importante que brinda una respuesta a un caso en particular.

1.3.1.2. Importancia de un sistema web

Según Cohen (2009, p.27), los sistemas de información y las tecnologías web se encuentran revolucionando la operación de la organización actual. A través de la utilización de estos se consigue un considerable cambio o mejora, pues facilita el proceso operativo de la organización, provee información de ayuda para los procesos relacionados a la toma de decisión y principalmente contribuye por medio de su implementación en la entidad el logro de alguna ventaja competitiva.
El sistema desarrollado en plataformas Web, tienen considerables diferencias con otros sistemas, lo cual da ventajas tanto para las organizaciones que lo emplean, como para los usuarios que utilizan el sistema. Estas diferencias se ven mostradas en los costos de las organizaciones, en la veloz obtención de la información, en el rendimiento de las tareas por parte de los empleados y en lograr una gestión completamente automatizada dentro y fuera de la organización.

En la actualidad las organizaciones se han convertido desde una perspectiva informática, para lograr facilidad y aligerar procesos que antes empleaban excesivo tiempo. Los Sistemas Web son un escalón más que las empresas anhelan

y procuran alcanzar en la administración de la información y en la fácil interacción con los empleados, permitiendo sistematizar diversos procesos, simplificándolos y potenciándolos, de modo que generen una mayor productividad a las actividades que se emplean en la empresa (Tacuri, 2015, p.53).

1.3.1.3. Dimensiones del sistema web

Según Ochoa (2017, p.24) señala como dimensiones:

> Fase 1: Análisis; que comprende el análisis de la información recolectada, como lo son el análisis de los participantes, así como el análisis de los requerimientos del usuario.
>
> Fase 2: Diseño; que comprende el diseño de la Entidad/Relación, así como el diseño de la navegación.
>
> Fase 3: Codificación: que abarca la especificación de las tecnologías utilizadas como lo son el lenguaje de programación, la base de datos y el programa de diseño, así como el procedo de codificación utilizado a cada una de las funcionalidades requeridas.
>
> Fase 4: Pruebas: que comprende el desarrollo de la efectividad del sistema, para lo cual se desarrollan pruebas durante el desarrollo, pruebas unitarias, y pruebas integradas.

1.3.1.4. Principios de los sistemas web

Según Ramírez (2017, p.38) el desarrollo de los sistemas web se sustenta en los siguientes principios:

> -Usabilidad: Para la Web, la usabilidad apareció a partir del principio y desarrollo de Internet como una red de intercomunicación. Surge en el área de investigación Interacción persona - ordenador como una ciencia que espera que los usuarios sientan comodidad al utilizar una aplicación determinada.
>
> -Seguridad: Se puede decir que uno de los puntos más críticos de la seguridad en Internet son las herramientas que interactúan de forma directa con los usuarios, en este caso los servidores web. Por otro lado, se ha encontrado que los inconvenientes detectados en el servicio web no

son provocados por fallas de ninguna de estas partes. Por el contrario, se ha demostrado que los problemas son producto de malas malas prácticas de los programadores. En el Sistema de Información se emplean seguridad mediante un login que tiene usuario y clave que por lo general permite accesos a cierta página como brinda privilegios a diferentes usuarios

-Disponibilidad: El indicador utilizado para medir la disponibilidad es el porcentaje de tiempo que emplea un sistema para realizar funciones para las que fue programado. Con respecto a los sistemas de mensajería, la disponibilidad es el porcentaje de tiempo empleado que el servicio de mensajería está disponible y en operatividad.

1.3.1.5. Características de los sistemas web

Según Berrospi y Pilar (2017, p.35) los sistemas web tienen las siguientes características:

-Logra generar códigos (lenguaje multiplataforma de licenciamiento libre).

-Se integran a cualquier motor de base de datos.

-Multidiomas: a partir del idioma original empleado para la ejecución de su utilización, manipulando un traductor, contribuye el trabajo con el propio sistema en una variedad de idiomas como sea requerido, registrando el cambio del contenido en un tiempo real.

Multiplataforma: dado que el servidor web recomendado para PHP es Apache (licenciamiento libre), y que tal servidor trabaja tanto en plataformas Linux con Windows, contribuye a que el sistema sea transportable a una plataforma a otra sin ejecutar algún cambio.

-Fácil mantenimiento: al tratarse de herramientas que tienden a tener capas espaciadas y bien determinadas, contribuye a ejecutar el mantenimiento de la aplicación a distancia, sobre el proyecto en su lugar de trabajo si fuera necesario.

-Orientado a Objetos: tanto el IDE, como el framework, están diseñados en clases, orientado a objetos para las interfaces de comunicación con el

cliente.

-Reporteador propio: la cual sujeta un diseñador de reporte propietario, el cual contribuye de manera simple a conceptualizar el reporte de salida con la conducción de un grupo, fórmula, etc. Creando una salida tanto en PDF como con planillas electrónicas.

-Multibrowser: en los equipos clientes, también puede trabajar tanto en Windows (Internet Explorer) como en Linux (Firefox).

-Diseño gráfico: la solución desarrollada con esta herramienta, cuenta con un estilo gráfico predefinido, contribuyendo a la generación de algo nuevo, redundando en una caracterización de las herramientas, no perdiendo el vínculo de equilibrio tanto de lo estético con el color.

-Fácil manejo: la forma que se ejecuta es intuitiva, uniendo un criterio al momento del desarrollo y la forma de desarrollo es intuitiva, unificando criterios a la hora del desarrollo y de la generación de código fuente.

-Generación automática a partir de una base de conocimiento de los procesos necesarios para la creación, actualización o eliminación de registros, con manejo transaccional de todas las operaciones.

-Auditable: Es el manejo de auditoría que se realiza de manera automática y parametrizable, contribuyendo a la registración solo de los logueos del usuario, hasta el circuito del mismo dentro del sistema.

-Seguridad: definición de "perfiles de acceso" a través del cual se admite o se niega el acceso y permiso de acción (alta, baja, modificar) al usuario del sistema.

-Ayuda: fácil definición de la ayuda, generando a medida que se desarrolla, la cual se traduce junto al resto del software generado.

1.3.1.5. Tipos de sistemas web

Según Castillo (2018, p.27) los sistemas web pueden ser de los siguientes tipos:

-Sistema web estático: En primer lugar, se debe conocer que este tipo de aplicaciones web muestran una tenue información y rara vez cambiar demasiado. Como norma general está desarrollada en el lenguaje HTML con estilos CSS. Además, también muestra en cierta parte de esta app Web algún objeto en movimiento como puede ser en un banner, GIF

animado, vídeo, etc. También puede ejecutarse una aplicación web con el script llamado jQuery y también con Ajax. Por otro lado, modificar los contenidos de las App estáticas no es fácil. Para lograrlo, habría que descargar el contenido HTML, luego modificarlo y finalmente subirlo al servidor web. Estas modificaciones sólo puede hacerlos el profesional web o la empresa de desarrollo contratada que programó e implementó la aplicación web. O buscar un profesional especializado para reemplazar a ese equipo. Algún ejemplo de aplicación web estática podría ser por ejemplo una web del tipo portafolio profesional o bien un curriculum vitae electrónico. Así una página de presentación de una organización podría tener este tipo de aplicación web para publicitar sus datos de contacto, etc.

b. Sistema web dinámica: Las App dinámica es mucho más compleja de acuerdo al tecnicismo. Emplea una base de datos para poder cargar alguna información, y este contenido se va actualizando cada vez que el usuario logra acceder a la web App. Habitualmente cuenta con paneles administrativos (llamado CMS) desde dónde los administradores pueden ir corrigiendo o modificando la información, ya sea un texto o imagen. Existen una infinidad de lenguajes de programación para desarrollo de aplicaciones web de tipo dinámicas. PHP y ASP son los más conocidos y empleados porque facilitan una buena estructuración del contenido web. La actualización tiene un proceso relativamente fácil y no necesita ingresar al servidor para cambiarlo. También permite implementar diversas funcionalidades como blogs o repositorios de datos. La vista web, y no solo el contenido puede modificarse al gusto del cliente.

-Sistema web E-commerce: Si la aplicación web es un negocio de ventas o comercio electrónico, se puede indicar que el desarrollo debe estar basado en los llamados comercios electrónicos conocidos como m-commerce o e-commerce. La implementación no es tan fácil porque debe facilitar pagos electrónicos por medio de tarjetas de crédito, débito, u otro medio de pago. En este ámbito el desarrollador tiene que crear un módulo para la administración de la tienda electrónica conocido como Backoffice. Este módulo le permitirá agregar, modificar, eliminar productos

adicionales, así como realizar seguimiento a los pagos de los clientes.

-Sistema web App: Es un tipo de portal o página principal desde el cual se puede acceder a las diversas secciones, departamentos o categorías. Contiene diferentes módulos: blogs, chats, correo electrónico, buscador, intranet, contenido más novedoso, etc.

-Sistema web animada: Las animaciones son realizadas utilizando la tecnología llamada FLASH. Es un tipo de programación que aporta animaciones y efectos. Además, facilita diseños más originales y modernos. Es una de las tecnologías más empleadas por programadores y diseñadores webs. La parte negativa de utilizar esta tecnología animada es el tema de posicionamiento web, debido a que no se logra una optimización SEO. Esta tecnología dificulta que los buscadores puedan identificar la web site.

-Sistema Web con "Gestor de Contenidos": Se refiere a los sitios webs donde el contenido es actualizado constantemente. Es requisito implementar un gestor de contenidos (CMS) por medio del cual el administrador pude realizar las modificaciones y actualizaciones del contenido. Estos gestores son amigables y tienen una interfaz intuitiva. Algunos ejemplos de estos son:

-WordPress: Es el más utilizado entre los gestores de contenidos. Existe una comunidad en la red que la respalda con tutoriales y manuales para la personalización. Además, es gratuito.

-Joomla: En segundo lugar, en el top CMS, muy cerda de WordPress. A pesar que no tiene demasiados usuarios como wordpress posee una comunidad muy activa.

-Drupal: Es un CSM open source. Es muy ligero y fácil de instalar, y posee una comunidad en crecimiento.

1.3.1.6. Ventajas del desarrollo de un sistema web

Según Blanco (2006, p.29) la implementación de un sistema o aplicación web para el desarrollo de un proceso origina muchas ventajas para la organización, entre las que se podemos decir:

- No es necesario una configuración especial ni actualizaciones en las

computadoras de los usuarios finales.

- La información se centraliza, es segura y es fácil realizar un respaldo.
- Las actualizaciones son inmediatas
- La información estará disponible las veinticuatro horas de todos los días.
- Los usuarios pueden acceder al sistema web desde cualquier dispositivo que cuente con un navegador web.
- Los requisitos para su ejecución son mínimos debido a que las operaciones se realizan del lado del servidor y no del cliente.

1.3.1.7. Arquitectura de desarrollo de sistemas webs

Según Espinoza (2013, p.33) un sistema de arquitectura más común es el sistema Modelo, Vista, Controlador. Esta arquitectura es un patrón utilizada para el desarrollo de aplicaciones web, se caracteriza porque separa en tres capas las vistas, la lógica de negocios y el modelo de la base de datos. Programar utilizando este patrón ayuda a mantener un código ordenado y facilita la modificación. Las empresas utilizan mucho esta arquitectura MVC debido a que los proyectos de desarrollo son más ordenados y el producto final se logra en un menor tiempo, además las actualizaciones son más fáciles de desarrollar, cabe resaltar que esta arquitectura debe apoyarse en una buena documentación para su fácil actualización.

Para Espinoza (2013, p.34) las partes del patrón MVC son:

-El modelo: Es una capa que se encarga que representa a la base de datos y que se conecta con ella para el almacenamiento de la información. Se recomienda que el modelo no sea dependiente de la base de datos. Además, desde la capa modelo se puede programar para que genere las tablas en la base de datos y así lograr su independencia del lenguaje SQL, es decir, si a futuro se desea migrar a otro proveedor de base de datos, no sería necesario crear las tablas puesto que el sistema lo crearía de forma automática. En esta capa las tablas son representadas por las llamadas Clases, y que tiene propiedades que representan a los campos en las tablas.

-El controlador: Se encarga de recepcionar los eventos de entrada y

gestiona o redirige las solicitudes hacia los módulos que contienen la lógica del negocio. Almacena un conjunto de reglas de gestión. Estas pueden ser peticiones para crear, actualizar o eliminar un registro en la base de datos.

-La vista: Es la capa encargada de recepcionar los datos y mostrarlos con un formato amigable para que el usuario pueda asimilar la información con facilidad. Generalmente cada vista está asociado a un específico controlador. Por ejemplo, para la vista mantenimiento de usuarios estará asociada a un controlador llamado usuario.

En este Modelo del mencionado patrón, se fijan las reglas que se ejecutarán para los datos de la aplicación; estos datos tienen que estar lógica y físicamente almacenados sobre un sitio web y con la respectiva seguridad que se necesite, por lo general se emplea solo una base de datos, la cual se detallará en la siguiente sección.

1.3.2. Gestión de la seguridad de la información

1.3.1.1. Definición de gestión de la seguridad de la información

Según Alexander (2007, p.48), conceptualiza a la seguridad como aquella regla técnica y actividad destinada a la prevención, protección y al resguardo de lo que se considera susceptible de hurto, daño o pérdida. Esta puede darse de forma individual, grupal o a nivel empresarial, por esto la información es el objeto principal que debe protegerse, resguardarse y recuperarse en las organizaciones.

Así mismo Aguirre y Aristizabal (2013, p.29), señalan que es entendida como una serie de datos que se encuentran organizados en dominio de una empresa que posee valor para la misma, independientemente de la manera que está a sido guardada o trasmitida (documentos escaneados, fotografías, audios, correos almacenados electrónicamente, etc.), de su origen (de la propia empresa o de un origen exterior) o de la fecha de creación.

Por lo tanto, por gestión de la seguridad de la información, según Ochoa (2017, p.47) se define como herramientas de gestión que contribuyen a saber, a la gestión y a la minimización del posible riesgo que atente contra la seguridad de la información en la Organización. Así mismo el modelo ISO 27001:20056 lo conceptualiza como la parte del sistema de gestión global, fundamentado en las orientaciones de algún riesgo de un negocio, en la cual le establezca, implemente, opere, monitoree, revise, mantenga y mejore la seguridad de información.

Para Areitio (2008, p.29) es el desarrollo de procesos que permiten asegurar la aptitud de un sistema de información en función a la forma en la que disuade, protege, detecta, responde y logra recuperar, proporciona la garantía de su activo en función de cómo reserva, protege, detecta y responde para su recuperación, proporciona la garantía de su activo en función a su reserva, integridad, disponibilidad, responsabilidad, autenticidad y fiabilidad, sin dejar de lado algún tipo de amenaza percibida.

1.3.1.2. Importancia de la gestión de la seguridad de la información

Guamán (2015, p.51) nos dice que la alta informatización de la sociedad actual ha conllevado el incremento de los llamados delitos informáticos, por lo que el establecimiento de un sistema informático es seguro si se puede confiar en él y si actúa de acuerdo a lo esperado. La seguridad dentro de los sistemas informáticos es entendida como la agrupación de planes, métodos y soluciones técnicas con el objetivo que la información que trata los sistemas informáticos se encuentre resguardado. Del mismo modo, busca establecer un plan de seguridad en el cual se definan las necesidades y objetivos en cuestiones de seguridad.

Ochoa (2015, p.42), toda empresa necesita de un sistema de seguridad de la información para resguardar sus activos más valiosos: la información y los procesos que la administran, asimismo de cada una de los empleados que hacen parte de los mismos siendo estos la columna vertebral para la empresa. La confidencialidad, integridad y disponibilidad de la información sensitiva, son elementos que resultan ser importantes para alcanzar el nivel de competencia, es rentable, y muestra una conformidad legal y empresarial requerida para obtener el objetivo de la empresa de manera que se asegure una rentabilidad económica. Es vital para la empresa implementar sistemas de gestión de seguridad de la información ya que no solo salvaguarda los activos principales, sino también se logra contar con asesorías necesarias y el apoyo de manera continua que fundamenta el ciclo PHVA 1 (planificar, hacer, verificar, actuar). Los sistemas de gestión de seguridad de la información ayudan a estar al nivel de una grande entidad que busca en la certificación de este tipo, una de la mayor ventaja competitiva con la que pueda lanzarse al mercado explorando así que mercados aún se encuentran disponibles.

1.3.1.3. Dimensiones de la gestión de la seguridad de la información

Según Ortiz y Martínez (2016, p.28) señala como dimensiones: confidencialidad, disponibilidad e integridad.

-Confidencialidad: Comprende las medidas para garantizar que el acceso confidencial está asegurado a quien debe. Consiste en gestionar qué usuario puede acceder a la información y restringir qué información confidencial se transmitirá a destinatarios no autorizados. Mediante esta propiedad la información no está habilitada o divulgada a organizaciones, personas u operaciones no autorizados (Alexander, 2007, p.35).

-Disponibilidad: Comprende las medidas para garantizar que la información estará servible en base a los requerimientos de la organización. Consiste en garantizar que los sistemas operen inmediatamente con un adecuado desempeño y garantizar la recuperación y protección del sistema para los casos de ataque o desastre informático. Esta es la propiedad de encontrarse disponible y servible

bajo solicitud de una entidad autorizada (Alexander, 2007, p.36).

-Integridad: Comprende las medidas para garantizar que la información este correcta y actualizada por el propietario de esta.
Consiste en garantizar que la información que se recepciona resulte ser idéntica a la información que se ha mandado, lo que representa que no existe ninguna alteración por error al ser transmitida o que muestre alguna modificación de manera intencional del contenido. Es la característica que tiene para preservar de forma exacta y total el activo (Alexander, 2007, p.36).

1.3.1.4. Elementos de la gestión de la seguridad de la información

Según el Modelo ISO 27001, (2005) indica que un sistema de gestión de seguridad de la información tiene que estar conformado por lo siguiente:

a. Alcance del sistema de gestión de seguridad de la información: que comprende en el contexto de una entidad que se encuentra subordinado a los sistemas de Gestión de Seguridad de la Información en la que incluye a la identificación clara de la dependencia, relación y límite que existe entre los alcances y aquella parte que no ha sido considerada (son en esos casos que el contexto de influencias de los sistemas de Gestión de Seguridad de la Información consideran como subconjuntos de la entidad como delegación, división, área, proceso, sistema o tarea concreta).

b. Identificación de activos: proviene de la identificación de todo activo diferente con la que cuenta la organización.

c. Política y objetivos de seguridad: es un documento que presenta contenidos genéricos que establecen compromisos de la dirección y de los enfoques de la organización que contribuyan a la gestión de la seguridad de la información.

d. Enfoque de evaluación de riesgos: Es la descripción de la metodología a utilizar (como se ejecuta la evaluación de la amenaza, vulnerabilidad, probabilidad de ocurrencia e impacto en relación al activo de información contenida dentro de los parámetros del alcance elegido), ejecución del criterio de aceptación de riesgo y fijación del nivel de riesgo aceptable.

e. Análisis y evaluación: son los estudios que resultan de la aplicación de

la metodología de evaluación que ha sido mencionada anteriormente al activo de la información de la entidad.

f. Opciones de tratamiento: luego de haber realizado su análisis y la evaluación de los riesgos, se debe resolver de cómo se debe se va a realizar el tratamiento teniendo en cuenta lo siguiente:

-Reducir: con el establecimiento del control para su atenuación (política, procedimiento, proceso y herramienta).

-Aceptar: se debe realizar la aceptación del riesgo en su respectivo nivel debido a que no resulta ser posible la ejecución de los tratamientos o porque terina siendo excesivamente costoso.

-Transferir: transferencia a terceros capacidad financiera 1 especialización indispensables para la administración de un riesgo adecuado.

- Evitar: impedir los riesgos eliminándolos de las actividades de la organización.

g. Enunciado de aplicabilidad: es un documento en la que se encuentra el objetivo de control y el control contemplado por los sistemas de Gestión de Seguridad de la Información. Este se fundamenta en el resultado del proceso de evaluación y tratamiento del riesgo, justificando la inclusión y exclusión.

h. Plan de tratamiento de riesgos: es un documento en la que se identifica la acción de la dirección, recurso, responsabilidad y prioridad para la gestión de riesgo de la seguridad de la información, teniendo en cuenta la conclusión obtenida en la evaluación de riesgo, del objetivo de control identificado, del recurso disponible, etc.

1.3.1.5. Objetivos de la gestión de la seguridad de la información

Para Guamán (2015, p.39) la función principal en seguridad informática es el bloqueo de los actos indeseables, y la prevención de actos que no se hayan estimado, de este modo si se originan hagan el mínimo daño. En este sentido se indican los objetivos que se deben realizar:

-Identificación de los usuarios: Hay diversas técnicas, entre las cuales se encuentran las claves (passwords), o sistemas más complejos como reconocimientos de voz, huella biométrica o la retina del ojo.

- Identificación de intrusos en la red: Se tiene que identificar y proceder sobre cualquier acceso no autorizada a un sistema. Tiene como finalidad la identificación de personas que no tengan permisos ni autorización en tiempo real, antes de que el sistema haya sido alterado considerablemente.
- Análisis de riesgo: Intenta medir el beneficio conseguido con la protección contra amenazas de seguridad. Los riesgos son funciones de la frecuencia con la que se inician dichas amenazas, fragilidad de la protección contra las mismas y las pérdidas potenciales que puedan darse en el caso que suceda alguna.
- Clasificación apropiada de los datos: En la administración de seguridad se reciben grandes cantidades de datos recogidos de los últimos esquemas de control generados a partir de las acciones que llevan a cabo los usuarios en el sistema. Resulta relevante para una adecuada inspección de la seguridad, el registro de datos convenientemente. Para así disminuir el tiempo de análisis.
- Control de las nuevas aplicaciones: Cuando se implementa nuevas aplicaciones se debe verificar que no ingrese nuevas brechas de seguridad especialmente si se instala con permisos de superadmin.
- Análisis de los accesos de los usuarios: Es requisito contar con un control para la identificación de intentos de acceso no autorizados.

1.3.1.6. Ciclo PDCA (Edward Deming)

Según Flores (2017, p.41) para la implementación de un sistema de Gestión de la seguridad de la información, es necesario la ejecución de operaciones que imprima un orden lógico para alcanzar un desarrollo ordenado durante todo el proceso. El modelo PDCA (Plan, do, check, act), o traducido al español: Planificar, hacer, verificar y actuar (PHVA), es una maniobra que tiene como objetivo el progreso constante de la calidad en cuatro etapas. Este modelo es muy popular para la implementación de sistemas de gestión, como los sistemas de gestión de la calidad. Diversas organizaciones lo implementan para la calidad administrativa de servicio, con la finalidad de perfeccionar y extender con los procesos de mejora continua. Por otro lado, para el establecimiento de los Sistemas de Gestión de la Seguridad informática, el ciclo PDCA resulta

pertinente por tratarse de una estrategia positiva para la organización y para el expediente que se requiera durante estos procesos.

1.3.2. Norma ISO/IEC 27001

1.3.2.1. Definición de la norma ISO/IEC 27001

Para Díaz (2010, p.39) la norma UNE-ISO/IEC 27001 está conformada por un "Sistema de Gestión de la Seguridad de la Información" y por un "Código de buenas prácticas de la gestión de la seguridad de la información", que fija las pautas a seguir para administrar la seguridad de la información de manera correcta y completa.

Por esto, Mesquida, Alcover y Mas (2010, p.41) comentan que este estándar internacional tiene una tendencia a dar modelos para la construcción, ejecución, operación, supervisión, exploración, sustento y mejora de un Sistema de gestión de Seguridad de la Información (SGSI).

Por otro lado, el Grupo ACMS Consultores (2017) indica que la norma 27001 ISO es una estándar internacional que evalúa el riesgo relacionado con toda la información que se administra en la organización y minimiza las amenazas originando más confianza entre sus usuarios.

De igual forma Frayssinet (2014, p.24) indica que la ISO IEC 27001 2013 es una norma de gestión de seguridad de la información, que describe un conjunto de requerimientos que facilitan aumentar la seguridad de la información.

Por eso Talavera (2015, p.37) indica que es una norma internacional diseñado como una guía para la evaluación, implementación, administración y mantenimiento de un Sistema de Gestión de Seguridad de la Información, a través del establecimiento de un grupo de requerimientos por cumplir con este motivo. Debido a su dirección orientada a las actividades del negocio, es un estándar general que se aplica a una diversidad de organizaciones, adaptándose a los diversos tipos de negocio y activos de información que éstas puedan tener. La

versión emitida el año 2013 tiene una estructura diferente según la norma definido por ISO/IEC para todos los estándares relacionados a sistemas de gestión, permitiendo la integración y operación conjunta entre las diversas normas de gestión publicadas por la mencionada entidad.

1.3.2.2. Características de la norma ISO/IEC 27001

Para Grupo ACMS Consultores (2017) indica como importantes particularidades:

A. El establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI) ISO 27001 notoriamente se direcciona en relación a nuevas medidas de organización que se tendrán que tomar en su organización para empezar a resguardar la información de posibles riesgos.

B. Estas medidas se tendrán que diseñar e instalar en una primera fase, estableciendo una política de los objetivos, de los procesos y de los procedimientos y posteriormente medir el rendimiento, revisando y haciendo una supervisión en las oficinas u áreas en donde se han implementado.

C. En la segunda fase se evaluará y se buscará mejorar con corrección o prevención, según sea el caso, de acuerdo al resultado obtenido de auditorías internas del sistema de gestión y de auditorías de revisión.

D. Las ventajas son muchas debido a que suman seguridad y además confianza y en cada una de las áreas de su organización. En resumen, dichos beneficios, mencionamos que implementando ISO 27001 logrará disminuir las amenazas de corrupción de la información, logrará implementar una metodología de gestión de la seguridad eficiente, facilitará continuar con las actividades tras haber padecido un ataque en la seguridad, reforzará a su organización ante eventuales peligros de pérdida de información y mejorará su imagen institucional en el mercado.

E. El estándar UNE-ISO/IEC 27001 Seguridad de la Información tiene afinidad con diversos sistemas de gestión que quizás tenga implementado en su organización como el sistema de gestión de la calidad según el estándar ISO 9001 y el sistema de gestión Medioambiental bajo el estándar ISO 14001, sistema de gestión de servicios de tecnologías de la información ISO 20000. etc.

1.3.2.3. Criterios generales en la aplicación de la norma ISO/IEC 27001

Para Ortiz y Martínez (2016, p.27) la implementación de un estándar ISO

necesita:

-Responsabilidad de cambio y adecuado soporte por parte de la empresa.

-Responsabilidad en los recursos y los tiempos de la empresa.

-Voluntad y profesionalidad por parte del implementador

La etapa de implementación efectúa modificaciones/crea procedimientos y normas además fijación de nuevas maneras de operar que afectan a las siguientes funciones de la empresa:

-Gerencia

-Recursos Humanos (Contratación y Formación)

-Compras

-Relaciones con Proveedores

-Seguridad Física

-Seguridad Lógica

-Infraestructuras

-Gestión de activos

-Gestión de las relaciones con los clientes

-Comunicación

Además la ISO27001:2013 se encuentra segmentada en 10 Capítulos

1. Objetivo y campo de aplicación: que abarca la compatibilidad y presentación con otros estándares.

2. Referencias normativas

3. Términos y definiciones: Que hacen referencia a la ISO27000 en la que se basa la nomenclatura.

4 Contexto de la organización: Comprende la descripción de la empresa y el alcance de la norma.

5 Liderazgo: Abarca el compromiso de la gerencia, actividades y normas de seguridad.

6 Planificación: Estudio del riesgo y objetivos de seguridad y planes para conseguirlos.

7 Soporte: Abarca la competencia, formación, fijación de mecanismos de comunicación así como requerimientos y control en la documentación

8 Operación: Abarca el diseño de las actividades y la administración del riesgo.

9 Evaluación del Desempeño: Abarca el rastreo de objetivos, la auditoría interna y revisión por la gerencia.

10 Mejora: Abarca el manejo de las inconformidades y acciones correctivas para la mejora continua.

1.3.2.4. Ventajas de la aplicación de la norma ISO/IEC 27001

Para el organismo TÜV SÜD (2013, p.24) la implementación del estándar presenta como destacables ventajas:

A. Disminución del riesgo: a través de una metodología de información con buena estructura y con reconocimiento global que identifica y reduce las diversas amenazas.

B. Protección de la información confidencial: de diversas amenazas como la copia ilegal, la pérdida de información, el quebrantamiento de confidencialidad, y asegurarse que su recuperación sea inmediata ante diversos ataques.

C. Implementar planes de continuidad empresarial: que garantiza que sus actividades seguirán en curso ante desastres naturales o causados por el hombre.

1.3.2.5. Importancia de la norma ISO/IEC 27001

Para Díaz (2010, p.43) el objetivo principal que se sigue es la administración de la seguridad de la información para obtener unos niveles de seguridad mínimos, y por ello es importante tener con un Sistema de Gestión de la Seguridad de la Información (SGSI), por medio de los actividades que se orientan a ser sistemáticos, documentados y reconocidos por la totalidad de la empresa de forma similar a como se diseñan los sistemas de gestión de la calidad según el estándar ISO 9001/ISO 14001, etc. La total seguridad es imposible al cien por ciento, aún si se destinen recursos materiales y además económicos, no se puede asegurar seguridad en su totalidad. La función que tiene un SGSI comprende en asegurar que el riesgo de la seguridad de la información sea reconocido, tomado, administrado y reducido por la organización de una manera.

1.3.2.6. Recomendaciones para la aplicación de la norma ISO/IEC 27001

Para Ortiz y Martínez (2016, p.45) se tienen que perseguir las siguientes recomendaciones:

R1: Obedecer la estructura de la norma: Lo primero que se sugiere a implementar es perseguir la propia estructura de la norma, como se mostrará es bastante práctica la mencionada distribución. Lo primero que debe ejecutar el implementador como parte de sus actividades es diseñar la estructura en una cantidad segura pero alcanzable por los componentes del SGSI

R2: Detectar al sponsor: En una implementación resulta relevante tener el mayor nivel posible de soporte por parte de la empresa. Cuanto mayor sea la altura en la cadena de jerarquía será mejor. Esto resulta esencial en la implementación y es responsabilidad del implementador detectar y obtener el mayor nivel de soporte durante la misma.

R3: Establecer el alcance: El alcance es el inicio de la implementación, conformará una parte del certificado que emitirá la organización auditora y tendrá a disposición de las partes interesadas que requieran conocer el contenido por el cual se ha emitido el certificado. De este modo el alcance es definido como un párrafo que tiene que contar con las siguientes características:

-Determinar la unidad o servicios certificados

- Determinar la ubicación geográfica donde se prestarán los servicios.

- Determinar los objetivos de la certificación

R4: Fijar el contexto de aplicación: Definido el alcance a certificar sobre éste es importante efectuar un estudio profundo sobre cómo se encuentra organizado siendo requerido:

-Realizar un estudio de la organización.

-Identificar el grado de aplicación.

R5: Política de Seguridad: Fijado el alcance y su estado de la seguridad la empresa tiene que elaborar una norma de seguridad que asegure los activos objeto del alcance. Dicha norma debe de tener las siguientes especificaciones:

-A lo máximo debe ocupar una página.

-Enfocarse en los pilares de la seguridad de la información que son confidencialidad, disponibilidad e integridad.

-Ser un documento de mayor nivel firmado por el sponsor o por la alta gerencia como manifestación de intenciones. Las cuales se rigen para la preservación de la seguridad.

-Mencionar la existencia de un objeto de control y defensa ante ataques.

R6: Definir las funciones: Definir las funciones de:

-Seguridad: los cuales conformarán parte del comité SGSI, como el Sponsor, el encargado de Seguridad Lógica, el encargado de Seguridad Física, operaciones, aplicaciones. Las funciones deben contar con las responsabilidades en seguridad de la información.

-Efectuar la normativa de seguridad, así como las leyes vigentes

-No divulgar la información confidencial de la organización

-Dueño de los procedimientos de seguridad

-Resguardar las copias de seguridad…

R7: Constituir el SGSI: Realizando las siguientes acciones:

-Oficializar el Acta a perseguir por parte del SGSI

-Objetivos, KPI y Cuadro de mando

-Supervisión por parte de la gerencia, determinar cuándo se efectuará una reunión de SGSI extraordinaria para la evaluación de los objetivos de seguridad.

-Acciones correctivas: qué actividades se ejecutarán si se necesitan acciones correctivas en el ámbito del SGSI

R8: Empezar un plan de agrupación. Empezar una estrategia en el cual todo trabajador relacionado a la norma de seguridad obtenga la formación precisa para su utilización y cumplimiento, guardando evidencia de:

-Su realización (convocatoria, firma de asistencia)

-Prueba de validez, en la cual son cuestionados aspectos de la norma luego de terminar cada tema para cada participante.

-Dar valor de la formación por cada participante

R9: Efectuar un estudio de Riesgos: Efectuar un estudio de riesgos que tenga en cuenta:

-SOA y cumplimiento de controles

-Amenazas en base a buenas prácticas tales como Magerit se puede utilizar para el cómputo aproximado del riesgo a través de la detección de las amenazas por activos y las amenazas estructurales o relacionadas al entorno que se hayan podido originar. Por otro lado, ante la detección de un posible riesgo, se tienen planeadas alternativas en función de quién lo asume diferirlo, aceptarlo, eliminarlo y establecer acciones mitigadoras.

R10: Aplicar Políticas de Activos: como lo son:

-Empleo de Activos: como se vio antes formar y fijar la política a los técnicos de soporte, incluso si es interno o externo.

-Administración del tiempo de vida de los activos: oficializar las actividades de compra, utilización y documentación, permisos, modificación, apagado/discontinuado, eliminación de información confidencial en los mismos, eliminación del inventario.

-Política de control de accesos: fijar política de control de accesos tanto físicos como lógicos, oficializando la revisión de los accesos lógicos y auditoría de los mismos con el fin de controlarlos. Esto abarca el tener que establecer una actividad de supervisión formal de éstos de manera organizada.

R11: Política de gestión de incidencias: como pueden ser:

-De Servicio: fijar, ligado al repositorio de datos de configuración la necesidad de operar por incidencias fijando convenios internos sobre el nivel de servicio adecuado para la reafirmación de entrega de transparencia al operar los equipos de soporte.

-De Seguridad: oficializar el incidente de seguridad y fijar su tratamiento, los incidentes de seguridad se solucionarán por los equipos de soporte, pero también serán revisados por el SGSI para detectar riesgos potenciales.

1.4. Formulación del problema

Problema general

¿Cuál será el efecto de un Sistema web en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos – La Molina?

Problemas específicos

Problemas específicos 1:

¿Cuál será el efecto de un Sistema web en la disponibilidad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos – La Molina?

Problemas específicos 2:

¿Cuál será el efecto de un Sistema web en la integridad de en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos – La Molina?

Problemas específicos 3:

¿Cuál será el efecto de un Sistema web en la confidencialidad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos – La Molina?

1.5 Justificación del estudio.

Este trabajo de investigación es importante realizar debido a los efectos que produce un sistema web para la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de Servicios Informáticos, este trabajo de investigación es conveniente realizar ya que estos últimos tiempos las empresas están teniendo problemas y muchos corren el riesgo o de un inadecuado uso de la información con la que cuenta la empresa, asimismo esta información si no es resguardada puede generar que la empresa se encuentre muchas veces vulnerable y

podrían llegar a personas ajenas a la empresa e incluso a los propios competidores quienes podrían emplear dicha información para su propio beneficio, partiendo de ello es importante contar con un sistema web para la seguridad, disponibilidad, integridad y confiabilidad de la información alineado a la norma ISO/IEC 27001 de manera que se haga más fácil la forma de evaluación de riesgo, la verificación de los mismos y el nivel de importancia de los activos. Este estudio servirá de base para futuras investigaciones y además para que los empresarios apliquen las tecnologías a su favor para salvaguardar información confidencial de sus empresas.

Este estudio además cuenta con su relevancia social ya que se quiere realizar un estudio experimental donde los beneficiarios directos son los trabajadores de la empresa de Servicios Informáticos., debido a la implementación de un sistema para la seguridad de la información alineado a la norma ISO/IEC 27001, asimismo los beneficiarios indirectos serían los usurarios o personas que requieren sus servicios y sabrán que su información es confidencial.

Las implicancias prácticas de este estudio son importantes porque va ayudar a resolver un problema real donde se ha observado que no se tiene el cuidado acerca de la seguridad de información en la empresa. En consecuencia, se aplicará un sistema web apropiado para salvaguardar esta información, lo que se podría considerar un aporte fundamental el sistema web para que otras empresas podrían aplicar para mejor su seguridad de la información alineado a la norma ISO/IEC 27001 todo ello con sus pasos.

El valor teórico de esta investigación es la información teórica valiosa del sistema web para la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001, se busca y se analiza en fuentes confiables tanto bibliotecas virtuales y presenciales para analizar las teorías que fundamentan las variables de estudio, la información que respalda todo ello citado en normas APA respetando los derechos de autor. La información obtenida contribuye a la revisión, desarrollo y sustento para una teoría. Esto facilita la creación y aplicación del experimento. A partir de los resultados observaremos la causa y el efecto que se produce lo que finalmente el investigador va proponer son las recomendaciones o hipótesis para futuros estudios que se realicen o desean profundizar.

La utilidad metodológica de este estudio de investigación permitirá la creación de un nuevo instrumento para la recolección y análisis de datos. Además, se logrará mejorar a través del experimento que es la aplicación de un sistema web para la gestión de la seguridad de la información alineado la norma ISO/IEC 27001, el aporte es que el investigador sigue una ruta metodología para lograr su trabajo y sus instrumentos y alcances pasando por proceso de confiabilidad y validez respectiva). (Hernández, Fernández y Baptista, 2014).

1.6 Hipótesis

El sistema web mejora significativamente la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos – La Molina

Hipótesis específicas

Hipótesis específica 1:
El Sistema web mejora significativamente la disponibilidad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informático – La Molina

Hipótesis específica 2:
El Sistema web mejora significativamente la integridad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos - La Molina

Hipótesis específica 2:
El Sistema web mejora significativamente la confidencialidad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos - La Molina

1.7. Objetivos

1.7.1. General

Determinar el efecto de un Sistema web en la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de servicios informático – La Molina

1.7.2. Específicos

Objetivo específico 1:

Analizar el efecto de un Sistema web en la disponibilidad en la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de servicios informáticos – La Molina

Objetivo específico 2:

Identificar el efecto de un Sistema web en la integridad en la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de servicios informáticos – La Molina

Objetivo específico 3:

Identificar el efecto de un Sistema web en la confidencialidad en la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de servicios informáticos – La Molina

I. MÉTODO

2.1. Diseño de investigación

El diseño de investigación es la planificación que se despliega para conseguir la información que se necesite en un estudio y contestar al planteamiento (Hernández, Fernández y Baptista, 2014, p.139).

El diseño en este estudio es el pre-experimental. Según Hernández, Fernández y Baptista (2014, p.141) en este diseño se manejan de forma deliberada, una o más variables independientes (causa). Luego se estudian los resultados de tal intervención sobre una o más variables dependientes (efectos).
El grupo experimental recepciona el estímulo.

La variable dependiente no se altera, por el contrario, es medida para observar el efecto que la intervención de la variable independiente tiene en ella. Esto se representa de la siguiente forma:

G E: 01 x 02

Donde:
G.E: Grupo experimental
X: Efectos del sistema Web
01: Pre test
02: Post test

En donde a un grupo se le aplica una evaluación antes de realizar algún tipo de estimulación experimental, luego se le aplica un tratamiento para luego aplicarle una evaluación final al estímulo. Se establece como parte inicial referencial para la observación del nivel en el que se encontraba el grupo en la variable dependiente previamente al estímulo. Dicho de otra forma, existe un perseguimiento al grupo. Por otro lado, el diseño no es conveniente para objetivos de fijar causalidad: no hay intervención ni grupo de comparación y tal vez actúen diversas fuentes de invalidación interna. Además, es riesgoso de elegir a un grupo anormal o que en el instante del experimento no se encontraba en su estado normal.

Tipo de estudio

Según su finalidad es aplicada

La resolución de problemas prácticos. El propósito de realizar aportaciones al conocimiento teórico es secundario. (Oyague y Sevilla, 2002, p. 185).

Según su profundidad es explicativa

Según Hernández, Fernández y Baptista (2014, p.102) es un estudio explicativo porque está dirigido a manifestar por la causa del evento y fenómeno físico o social. Se orienta en darle explicación porque tiende a ocurrir fenómenos y en qué condición se expresa, o por qué se vincula dos o más variables.

El estudio explicativo tiende a expandirse más allá de la descripción de un concepto o fenómeno o del establecimiento de la relación entre definiciones, lo que significa, está dirigido a contestar por la causa del evento y fenómeno físico o social. Tal como su propio nombre lo indica, el interés tiende a centrarse en la explicación de lo que ocurre en fenómenos y en una condición que se expresa por qué se vincula dos o más variables.

Enfoque de investigación

Dado el trabajo de investigación es cuantitativo porque observa la realidad, la describe plantea la problemática, y recoge información aplica un sistema para mejorar y después lo interpreta mediante la estadística descriptiva e inferencial con datos numéricos.

2.2. Variable, operacionalización

2.2.1 Definición conceptual

Variable independiente (VI): Sistema web

Para Berrospi y Pilar (2017, p.45) conceptualiza como una serie de distintas fracciones o compendios que se hallan constituidos y vinculados entre sí, que tienden a interactuar entre sí para conseguir las metas. El sistema recibe datos que constituye la entrada, y provee la salida que sería la información.

Definición operacional

La aplicación web que se creará con el propósito de salvaguardar la seguridad de la información alineado a la norma ISO/IEC 27001, tomando en cuenta las fases que son 1: Análisis, -Fase 2: Diseño, -Fase 3: Codificación, Fase 4: Pruebas; todo esto permitirá tener la seguridad de la información en la empresa de Servicios Informáticos ya que hoy en día por la competencia existen riesgos y amenazas externas o internas al robo de información que maneja cada empresa.

Variable independiente (VD): Gestión de la seguridad de la información

Definición conceptual

Alexander (2007, p.73) conceptualiza a la seguridad como una regla técnica o actividad cuyo objetivo central es la que busca prevención, protección y al resguardo de lo que se considera dispuesto de hurto, pérdida o avería. Este puede darse de forma personal, grupal o empresarial. Por este motivo es considerado como un recurso importante el cual debe de ser protegido, resguardado y recuperado de en las organizaciones.

Definición operacional

La seguridad en las empresas es necesaria para salvaguardar la información y que no caiga en manos de personas que podrían hacer daño.

Tabla 2

Operacionalización de la variable gestión de la seguridad

Variable Dependiente	Definición conceptual	Definición operacional	Dimensión	Indicador	Instrumento	Escala
Gestión de la seguridad de la información	Terry (2017, p.75) se define la gestión como un proceso que consiste en la planificación, organización, accionar y controlar, realizado para determinar y llevar a cabo los objetivos mediante el uso de personas y recursos.	La seguridad de la información en las empresas se considera que es conjunto de responsabilidades, procesos, procedimientos y recursos que establece la alta dirección con el propósito de dirigir y controlar la seguridad de los activos de información y asegurar la continuidad de la operatividad de la empresa. Se evalúa a través de sus dimensiones en un cuestionario.	Disponibilidad de la información	- **% Reportes entregados en el plazo establecido** Reportes entregados en el plazo establecido **Valor =** _____ *** 100** Total de reportes	Observación	Razón
			Integridad de la información	- **% Reportes Integros generados** Reportes Íntegros generados **Valor=** _____ ***100** Total de reportes		Razón
			Confidencialidad de la información	- **% Reportes confidenciales Entregados Correctamente** **Reportes confidenciales entregados correctamente** **Valor=** ***100** **Total de reportes**		Razón

Fuente: Elaboración propia del investigador.

2.3 Población y muestra

Población

Vara (2012, p.56), lo define como un conjunto de personas que cuentan con rasgos comunes, ubicándolo en un mismo contexto y tiende a variar después de un periodo.

La población es una serie de individuos que presentan una serie de características en común, se ubican en el mismo entorno y varían en el transcurso del tiempo (p. 221).

En la presente investigación, la población está conformada por la cantidad de informes diarios de backup de clientes, siendo estos una cantidad de 30 informes en un periodo de 30 días.

Muestra

Guerrero, Victoria y Curieses (2007, p.24) definen a la muestra como el subconjunto de la población que es seleccionada en función a ciertos procedimientos estadísticos. Estos son denominados “teoría de muestreo”.

Según Muñoz (2011, p.117) “a veces es imposible realizar la recolección de todos los datos que afectan un fenómeno, ni es posible investigar todos los elementos del ámbito geográfico relacionados al estudio, ya que, no se puede operar y a su vez tendría un costo muy alto. Así que, en estos casos es mejor realizar una recopilación parcial de los datos, escogiendo algunos elementos representativos del universo de estudio.”

De lo descrito anteriormente, en la presente investigación consideró como muestra a la cantidad total de la población.

Muestreo

Abramson (1990, p.74) señala que el muestreo probabilístico es cuando cada unidad individual de la población total (o unidad muestral) posee una probabilidad conocida de resultar elegida. Ello permite realizar generalizaciones sobre la población origen con una precisión y confianza medibles".

Para esta investigación se optó por no seleccionar ningún tipo de muestreo. Esto porque se utilizó la misma cantidad de unidades muestrales que integraron la población.

2.5 Técnicas e instrumentos de recolección de datos, validez y confiabilidad

2.5.1. Técnicas de recolección de datos

Observación

Ñaupas, H., Mejía, E., Novoa, E. & Villagómez, A. (2013, p.51) consideran que la observación es la dinámica en la que se establece un contacto directo del sujeto cognoscente y el objeto o fenómeno por conocer. Esto se da con la intervención de los sentidos, principalmente la vista, el oído, el tacto y el olfato. Para la realización del presente trabajo se ha visto conveniente el uso de la técnica de recojo de datos denominada observación. Esta decisión se respalda en que se tendrá contacto directo con las personas involucradas y el fenómeno a estudiar.

2.5.2 Instrumentos de recolección de datos

Ficha de Registro

Vara (2012, p.57), nos dice que la ficha de registro es un instrumento que facilita el registro de todas las observaciones efectuadas en el proceso de recopilación de datos para luego medir los indicadores plasmándolo en un formato. En esta investigación se vio conveniente el uso de este instrumento para ambos indicadores.

2.6 Métodos de análisis de datos

Vara (2012, p.62), Para el análisis y proceso estadístico se hará uso del software estadístico SPSS-22, para ello previamente los datos serán llevados a la hoja de cálculo Excel 2016 data donde se encuentren todos los códigos de los sujetos muéstrales.

Después de ejecutar la recolección de información por medio de la aplicación de los instrumentos a los que integra la muestra se necesita seguir la siguiente secuencia:
Data de resultados: En esta fase se tendrá que llenar una data con cada resultado que ha sido obtenidos en cada instrumento teniendo en cuenta la valoración asignada por cada opción de respuesta en la hoja de Excel.

Tabulación e interpretación de los resultados: En esta fase se estructurarán cada una de las tablas y figuras de acuerdo a los datos obtenidos luego del procesamiento teniendo en cuenta tanto la frecuencia absoluta y porcentual y la medida de tendencia central, de manera que se pueda efectuar cada una de las interpretaciones.

El método de análisis de datos que se empleará será del tipo cuantitativo y se hará uso de la estadística descriptiva, utilizando varianza, mediana, tablas y gráficos estadísticos que nos permitirá comparar la variable utilizada. Por otro lado, se utilizará el software estadístico llamado SPSS para el análisis de datos. Para el preámbulo de la comprobación de la hipótesis se ejecutará una prueba de normalidad de los datos.

2.7 Aspectos éticos

La investigación velará por las siguientes consideraciones éticas:

- Se acepta en plenitud participar en la investigación.
- Se respetará la veracidad de los resultados y de los datos suministrados por los usuarios de las empresas involucradas.
- Se hará uso de las normas APA para citar a los autores que fueron usados para respaldar el presente proyecto, mencionándolos en las referencias bibliográficas.
- Se mantendrá en reserva la información confidencial a la que se ha podido tener acceso en la empresa.
- Se mantendrá en absoluta reserva la identidad del nombre de la empresa en la cual se realizan las practicas, debido a la estrictica y rigurosa confidencialidad que se maneja en dicha empresa lo cual puede infringir sus políticas de seguridad.

III. RESULTADOS

3.1 Análisis Descriptivo

Para la presente investigación se utilizó un sistema web para determinar su efecto en el proceso de disponibilidad, integridad y confidencialidad de los reportes de backup en la gestión de seguridad de la información; para ello se empleó un pre test que hizo posible conocer las condiciones primarias de sus indicadores; posteriormente se implementó el sistema Web y nuevamente se registraron datos de sus indicadores. Los resultados descriptivos de estas medidas se observan en las siguientes tablas.

Indicador: Porcentaje Reportes entregados en el Plazo establecido

Tabla 3: Medidas descriptivas del Porcentaje de Reportes entregados en el plazo establecido antes y después de implementación del sistema Web.

	N				
	Válido	Perdidos	Media	Mínimo	Máximo
% Reportes entregados en el plazo establecido-PRETEST	30	0	72,3340	40,00	100,00
% Reportes entregados en el plazo establecido - POSTEST	30	0	97,9443	75,00	100,00

Para la investigación se consideró el porcentaje de Reportes entregados en el plazo establecido durante un mes, con relación a los datos obtenidos de antes de la implementación del sistema web se encontró una media de 72.33%, mientras que para los datos obtenidos después de la implementación del sistema web se encontró una media de 97.94%, esto indica una diferencia importante antes y después de la implementación del sistema; asimismo, el porcentaje mínimo de reportes entregados a tiempo fue de 40% antes y 75% después (ver Figura 1).

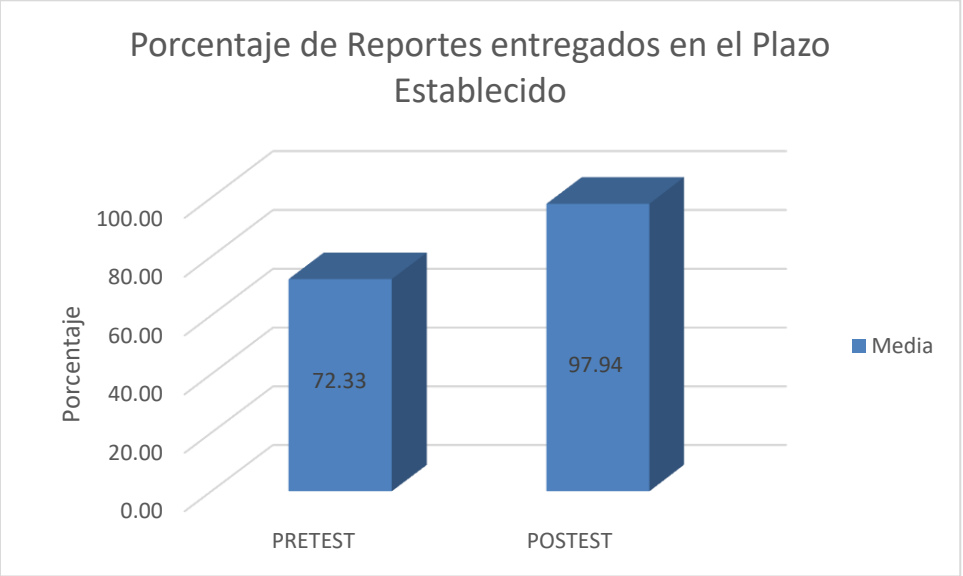


Figura 1: Porcentaje de Reportes entregados en el plazo establecido antes y después de implementado el sistema web.

Indicador: Porcentaje de Reportes Íntegros generados

Tabla 4. Medidas descriptivas del Porcentaje de Reportes Íntegros generados antes y después de implementado el sistema web.

	N				
	Válido	Perdidos	Media	Mínimo	Máximo
% Reportes Íntegros generados - PRETEST	30	0	74,0557	50,00	100,00
% Reportes Íntegros generados - POSTEST	30	0	97,9443	75,00	100,00

Para la investigación se consideró el Porcentaje de Reportes Íntegros generados durante un mes, con relación a los datos obtenidos de antes de la implementación del sistema Web, se encontró una media de 74.05 % mientras que para los datos obtenidos después de la implementación del sistema web se encontró una media de 97.94 % esto indica una diferencia importante antes y después de la implementación del sistema web; asimismo, el Porcentaje de Reportes Íntegros generados fue del 50% antes y 75% después (ver Figura 2).

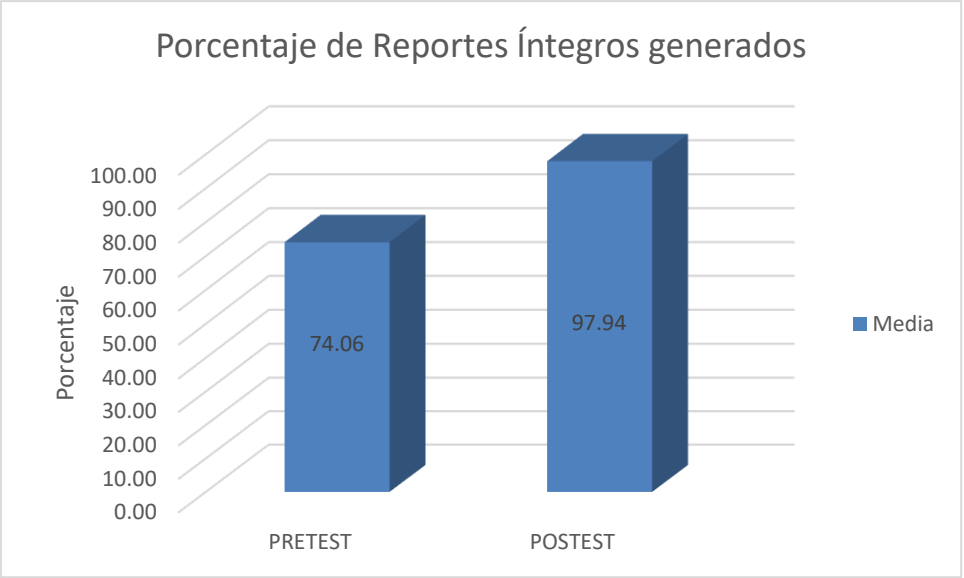


Figura 2: Porcentaje de Reportes Íntegros generados antes y después de implementado el sistema web.

Indicador: Porcentaje Reportes Confidenciales Entregados Correctamente

Tabla 5. Medidas descriptivas del Porcentaje Reportes Confidenciales Entregados Correctamente antes y después de implementado el sistema web.

	N				
	Válido	Perdidos	Media	Mínimo	Máximo
% Reportes Confidenciales Entregados Correctamente - PRETEST	30	0	77,3890	50,00	100,00
% Reportes Confidenciales Entregados Correctamente - POSTEST	30	0	96,6663	66,67	100,00

Para la investigación se consideró el Porcentaje Reportes Confidenciales Entregados Correctamente durante un mes, con relación a los datos obtenidos de antes de la implementación del sistema Web, se encontró una media de 77.39 % mientras que para los datos obtenidos después de la implementación del sistema web se encontró una media de 96.67 % esto indica una diferencia importante antes y después de la implementación del sistema web; asimismo, el Porcentaje Reportes Confidenciales Entregados Correctamente fue del 50% antes y 66.67% después (ver Figura 2).

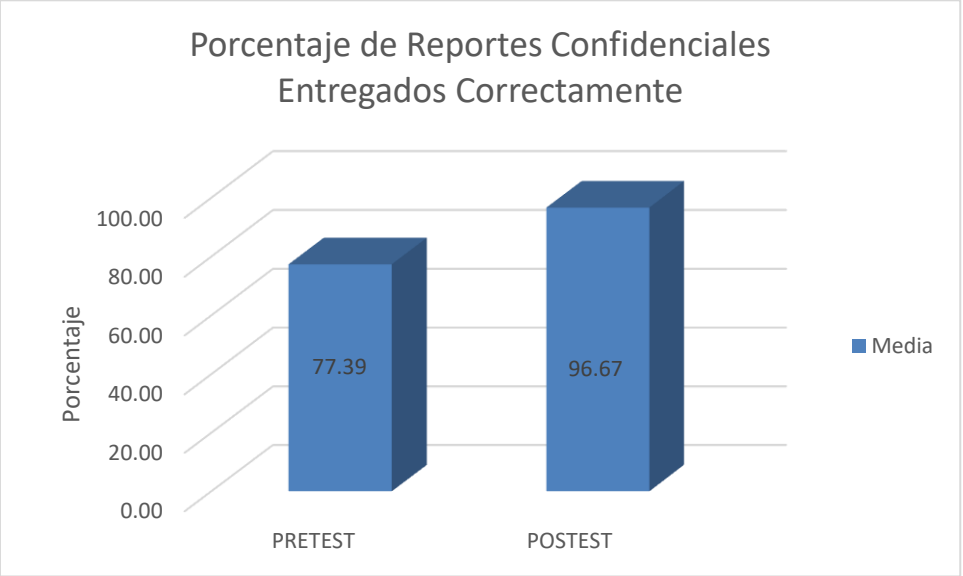


Figura 3: Porcentaje Reportes Confidenciales Entregados Correctamente antes y después de implementado el sistema web.

3.2 Análisis inferencial

3.2.1 Prueba de Normalidad

Con el objetivo de seleccionar la prueba de hipótesis; los datos fueron sometidos a la comprobación de su distribución, específicamente si los datos contaban con distribución normal.

Bernal (2014, p.20) menciona que "utilizaremos la Prueba de Kolmogorov-Smirnov si hay más de 50 unidades de análisis o la de Shapiro-Wilk si hay menos de 50 unidades de análisis".

Indicador: Porcentaje de Reportes entregados en el plazo establecido

Con el objetivo de seleccionar la prueba de hipótesis; los datos fueron sometidos a la comprobación de su distribución, específicamente si los datos de porcentaje de Reportes entregados en el plazo establecido contaban con distribución normal. Se utilizó la prueba de Shapiro-Wilk para las 30 unidades de análisis (ver tabla 5).

Ho: Los datos tienen un comportamiento normal.
Ha: Los datos no tienen un comportamiento normal.

Tabla 5. Prueba de normalidad de Porcentaje de Reportes entregados en el plazo establecido antes y después de implementado el sistema web.

	Shapiro-Wilk		
	Estadístico	gl	Sig.
% Reportes entregados en el plazo establecido - PRETEST	,915	30	,019
% Reportes entregados en el plazo establecido - POSTEST	,361	30	,000

Los resultados de la prueba indican que el Sig. de la muestra de Porcentaje de Reportes entregados en el plazo establecido, antes fue de 0.019, cuyo valor es menor que 0.05 (nivel de significancia), entonces se rechaza la hipótesis nula, por lo que indica que los datos no se distribuyen normalmente.

De manera similar, los resultados de la prueba indican que el Sig. de la muestra de Porcentaje de Reportes entregados en el plazo establecido, después fue de 0.000, cuyo valor es menor que 0.05 (nivel de significancia), entonces se rechaza la hipótesis nula, por lo que indica que los datos no se distribuyen normalmente.

En la Figura 3 se representa un histograma de los valores obtenidos para el indicador “Porcentaje de Reportes entregados en el plazo establecido” antes de implementar el sistema web, teniendo una media de 72.3 en el valor porcentual. Además, en el eje horizontal observamos los valores del Porcentaje de Reportes entregados en el plazo establecido y en el eje vertical se puede observar el número de veces que se representan los valores porcentuales en un intervalo, es decir, la frecuencia. Se puede apreciar como las barras no guardan proporción a la curva de distribución normal y esto es debido a que no existe distribución normal (ver Figura 3).

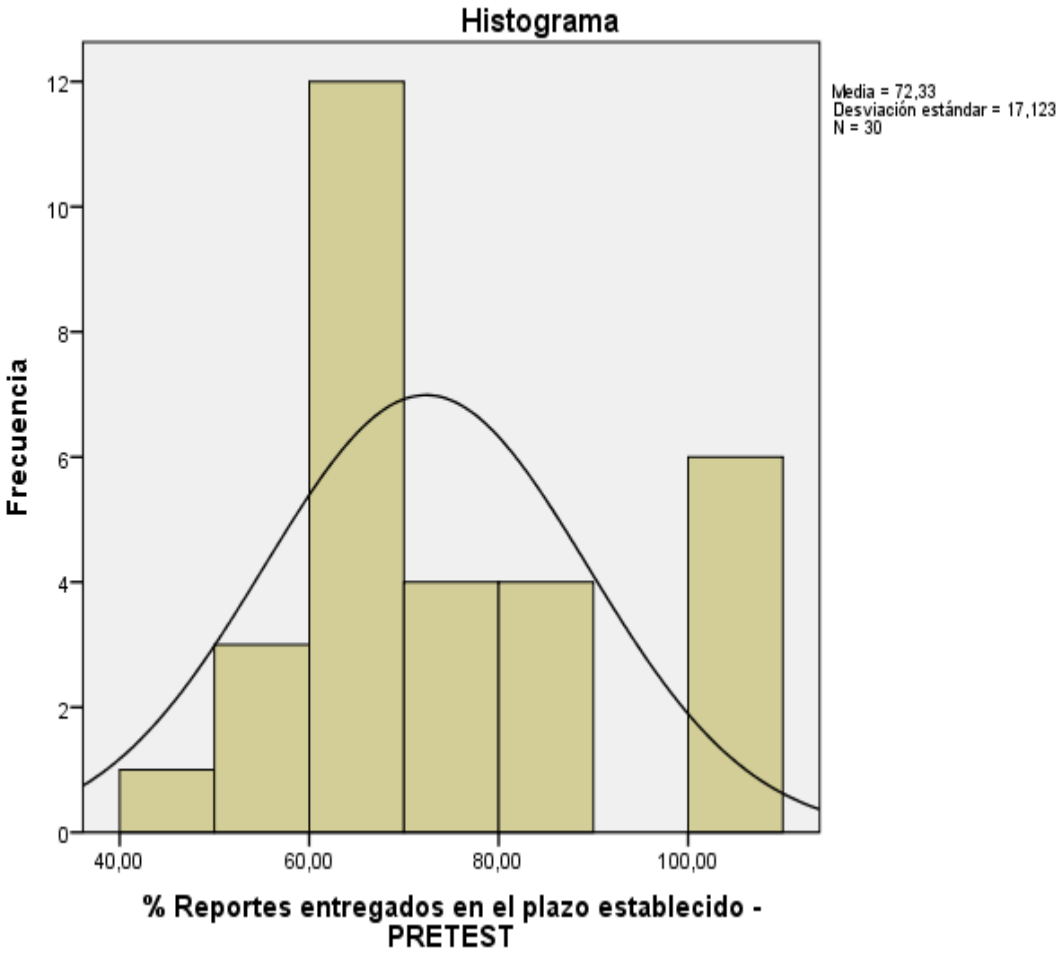


Figura 3: Prueba de Normalidad de Porcentaje de Reportes entregados en el plazo establecido antes de implementado el Sistema web.

En la Figura 4 se representa un histograma de los valores obtenidos para el indicador “Porcentaje de Reportes entregados en el plazo establecido” después de implementar el sistema web, teniendo una media de 97.94 en el valor porcentual. Además, en el eje horizontal observamos los valores del porcentaje de Reportes entregados en el plazo establecido y en el eje vertical se puede observar el número de veces que se representan los valores porcentuales en un intervalo, es decir, la frecuencia. Se puede apreciar como las barras no guardan proporción a la curva de distribución normal y esto es debido a que no existe distribución normal (ver Figura 4).

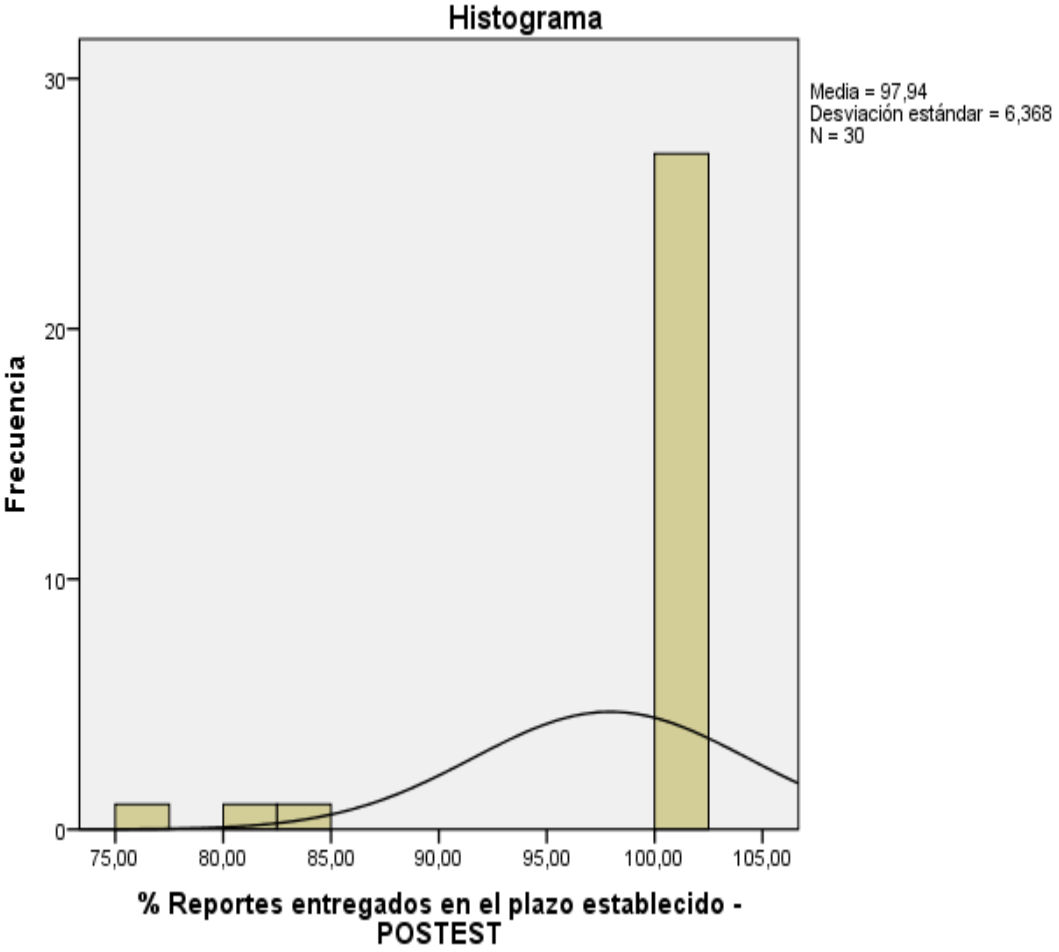


Figura 4: Prueba de Normalidad de porcentaje de Reportes entregados en el plazo establecido después de implementado el Sistema web.

Indicador: Porcentaje de Reportes Íntegros generados

Con el objetivo de seleccionar la prueba de hipótesis; los datos fueron sometidos a la comprobación de su distribución, específicamente si los datos de Porcentaje de Reportes Íntegros generados contaban con distribución normal. Se utilizó la prueba de Shapiro-Wilk para las 30 unidades de análisis (ver tabla 6).

Ho: Los datos tienen un comportamiento normal.
Ha: Los datos no tienen un comportamiento normal.

Tabla 6. Prueba de normalidad de Porcentaje de Reportes Íntegros generados antes y después de implementado el sistema web.

	Shapiro-Wilk		
	Estadístico	gl	Sig.
% Reportes Íntegros generados - PRETEST	,863	30	,001
% Reportes Íntegros generados - POSTEST	,361	30	,000

Los resultados de la prueba indican que el Sig. de la muestra de Porcentaje de Reportes Íntegros generados antes fue de 0.001, cuyo valor es menor que 0.05 (nivel de significancia), entonces se rechaza la hipótesis nula, por lo que indica que los datos no se distribuyen normalmente.

De manera similar, los resultados de la prueba indican que el Sig. de la muestra de Porcentaje de Reportes Íntegros generados después fue de 0.000, cuyo valor es menor que 0.05 (nivel de significancia), entonces se rechaza la hipótesis nula, por lo que indica que los datos no se distribuyen normalmente.

En la Figura 5 se representa un histograma de los valores obtenidos para el indicador “Porcentaje de Reportes Íntegros generados” antes de implementar el sistema informático, teniendo una media de 74.06 %. Además, en el eje horizontal observamos los valores del Porcentaje de Reportes Íntegros generados y en el eje vertical se puede observar el número de veces que se representan los valores en un intervalo, es decir, la frecuencia. Se puede apreciar como las barras no guardan proporción a la curva de distribución normal y esto es debido a que no existe distribución normal (ver Figura 5).

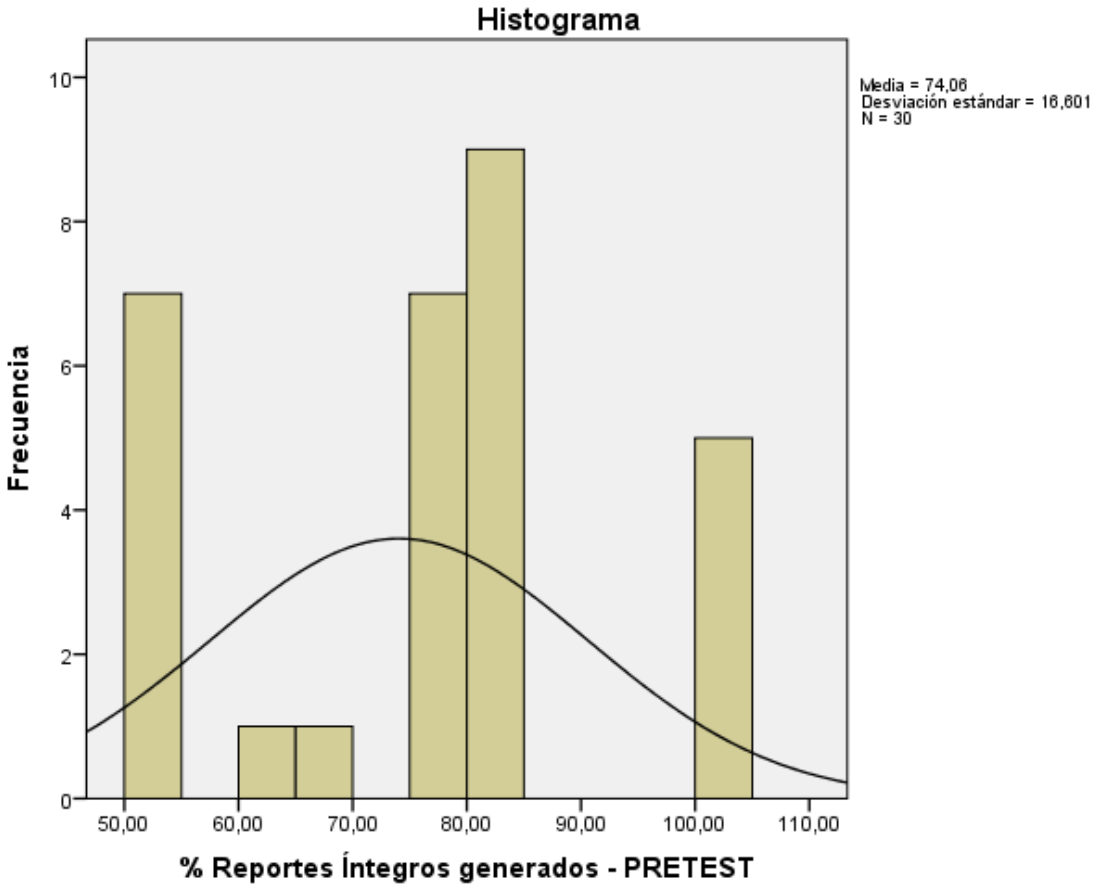


Figura 5: Prueba de Normalidad de Porcentaje de Reportes Íntegros generados antes de implementado el Sistema web.

En la Figura 6 se representa un histograma de los valores obtenidos para el indicador “Porcentaje de Reportes Íntegros generados” después de implementar el sistema web, teniendo una media de 97.94 %. Además, en el eje horizontal observamos los valores del Porcentaje de Reportes Íntegros generados y en el eje vertical se puede observar el número de veces que se representan los valores en un intervalo, es decir, la frecuencia. Se puede apreciar como las barras no guardan proporción a la curva de distribución normal y esto es debido a que no existe distribución normal (ver Figura 6).

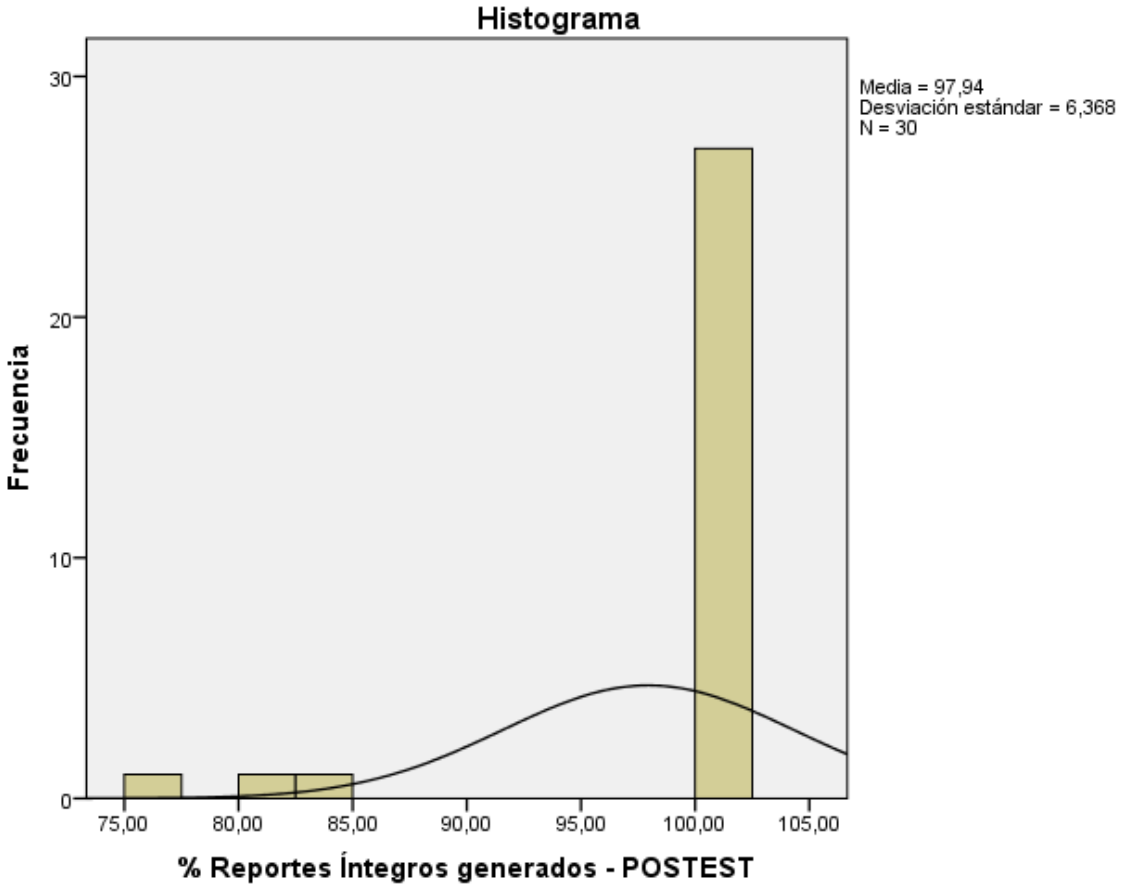


Figura 6: Prueba de Normalidad de Porcentaje de Reportes Íntegros generados después de implementado el Sistema web.

Indicador: Porcentaje Reportes Confidenciales Entregados Correctamente

Con el objetivo de seleccionar la prueba de hipótesis; los datos fueron sometidos a la comprobación de su distribución, específicamente si los datos de Porcentaje Reportes Confidenciales Entregados Correctamente contaban con distribución normal. Se utilizó la prueba de Shapiro-Wilk para las 30 unidades de análisis (ver tabla 6).

Ho: Los datos tienen un comportamiento normal.
Ha: Los datos no tienen un comportamiento normal.

	Shapiro-Wilk		
	Estadístico	gl	Sig.
% Reportes Confidenciales Entregados Correctamente - PRETEST	,812	30	,000
% Reportes Confidenciales Entregados Correctamente - POSTEST	,471	30	,000

Tabla 7. Prueba de normalidad de Porcentaje Reportes Confidenciales Entregados Correctamente antes y después de implementado el sistema web.

Los resultados de la prueba indican que el Sig. de la muestra de Porcentaje Reportes Confidenciales Entregados Correctamente, antes fue de 0.000, cuyo valor es menor que 0.05 (nivel de significancia), entonces se rechaza la hipótesis nula, por lo que indica que los datos no se distribuyen normalmente.

De manera similar, los resultados de la prueba indican que el Sig. de la muestra de Porcentaje Reportes Confidenciales Entregados Correctamente después fue de 0.000, cuyo valor es menor que 0.05 (nivel de significancia), entonces se rechaza la hipótesis nula, por lo que indica que los datos no se distribuyen normalmente.

En la Figura 6 se representa un histograma de los valores obtenidos para el indicador “Porcentaje Reportes Confidenciales Entregados Correctamente” antes de implementar el sistema informático, teniendo una media de 77.39 %. Además, en el eje horizontal observamos los valores del Porcentaje Reportes Confidenciales Entregados Correctamente y en el eje vertical se puede observar el número de veces que se representan los valores en un intervalo, es decir, la frecuencia. Se puede apreciar como las barras no guardan proporción a la curva de distribución normal y esto es debido a que no existe distribución normal (ver Figura 6)

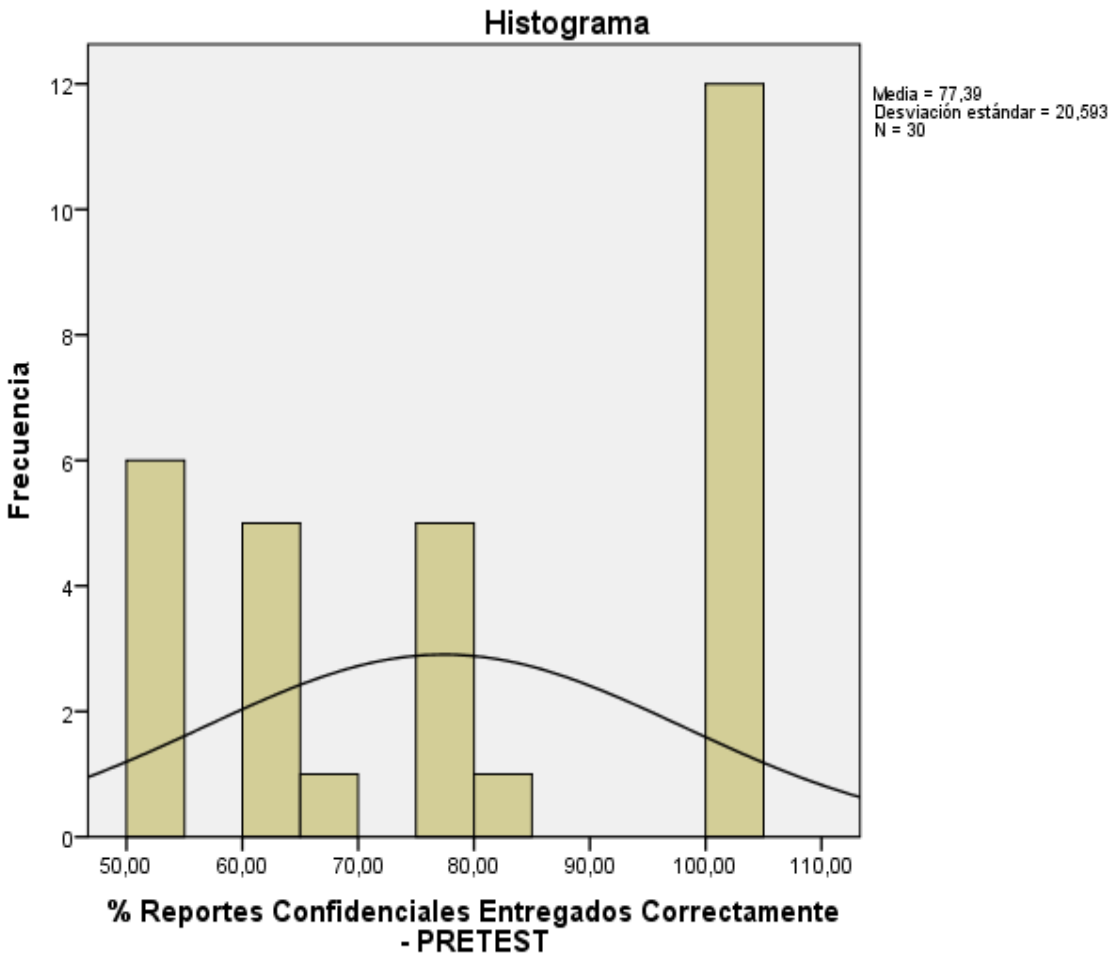


Figura 6: Prueba de Normalidad de Porcentaje Reportes Confidenciales Entregados Correctamente antes de implementado el Sistema web.

En la Figura 7 se representa un histograma de los valores obtenidos para el indicador “Porcentaje Reportes Confidenciales Entregados Correctamente” después de implementar el sistema web, teniendo una media de 96.67 %. Además, en el eje horizontal observamos los valores del Porcentaje Reportes Confidenciales Entregados Correctamente y en el eje vertical se puede observar el número de veces que se representan los valores en un intervalo, es decir, la frecuencia. Se puede apreciar como las barras no guardan proporción a la curva de distribución normal y esto es debido a que no existe distribución normal (ver Figura 7).

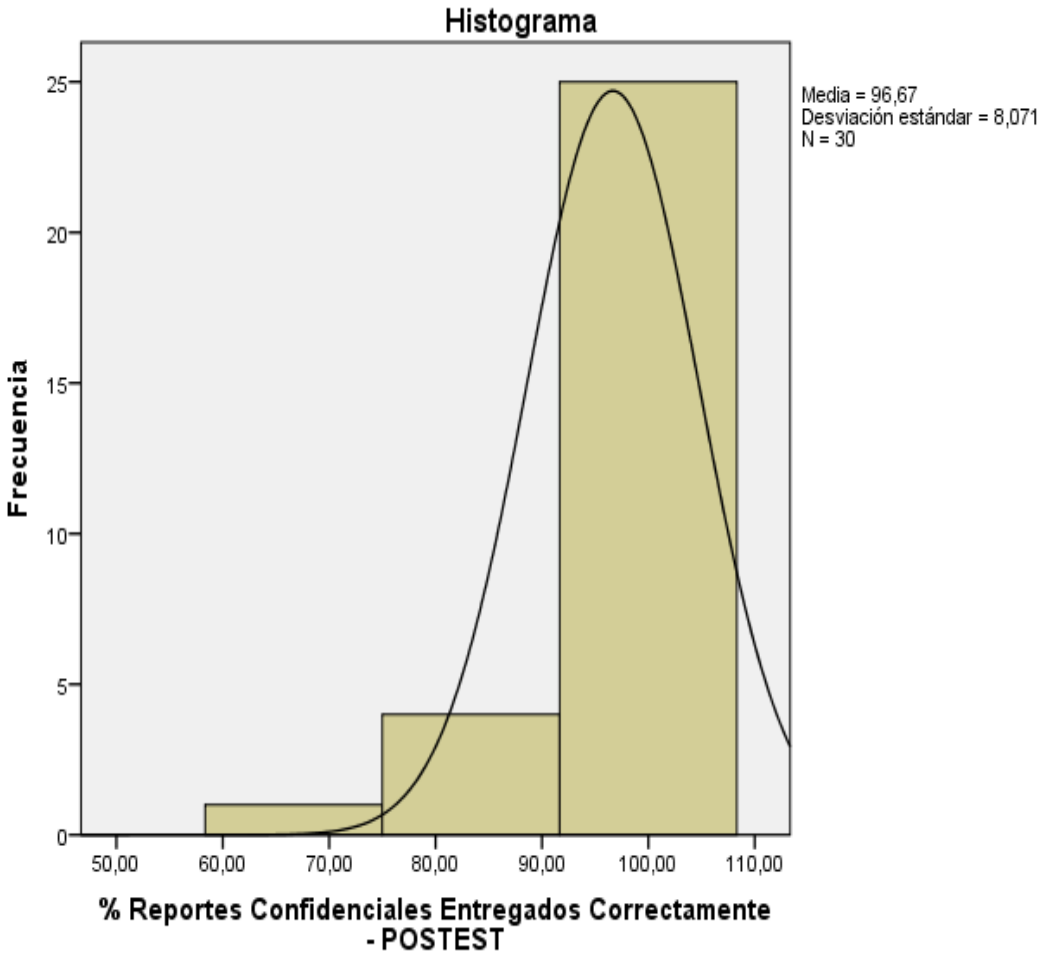


Figura 7: Prueba de Normalidad de Porcentaje Reportes Confidenciales Entregados Correctamente después de implementado el Sistema web.

3.2.2 Prueba de Hipótesis

Como la prueba de normalidad, dio como resultado que los datos de los indicadores “Porcentaje de Reportes entregados en el plazo establecido”, “Porcentaje de Reportes Íntegros generados” y “Porcentaje Reportes Confidenciales Entregados Correctamente” no cumplen el requisito de distribución normal se utilizó la prueba de Wilcoxon para muestras relacionadas (ver tablas 7, 8, 9, 10,11,12 y 13).

A. Hipótesis de investigación 1

H1: El Sistema web mejora significativamente la disponibilidad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos – La Molina

Indicador: Porcentaje de Reportes entregados en el plazo establecido

Hipótesis Estadística

Definición de Variables:
PREPEa: Porcentaje de Reportes entregados en el plazo establecido antes de implementar el sistema web.
PREPEd: Porcentaje de Reportes entregados en el plazo establecido después de implementar el sistema web.

H1o: El uso del sistema web no aumenta el porcentaje Reportes entregados en el plazo establecido.

$$H1o: PREPEd \leq PREPEa$$

H1a: El uso del sistema web si aumenta el porcentaje de Reportes entregados en el plazo establecido.

$$H1a: PREPEd > PREPEa$$

Tabla 8. Diferencia significativa en el Porcentaje de Reportes entregados en el plazo establecido antes y después de implementado el sistema web.

	Z	Sig. asintótica (bilateral)
% Reportes entregados en el plazo establecido - POSTEST - % Reportes entregados en el plazo establecido - PRETEST	-4,305[b]	,000

a. Prueba de Wilcoxon de los rangos con signo

b. Se basa en rangos negativos.

Los resultados de la prueba de Wilcoxon muestran que el P valor es de 0.000 menor a 0.05 lo que significa que existe diferencia significativa en el porcentaje de Reportes entregados en el plazo establecido antes y después de implementado el sistema web.

Tabla 9. Rangos de porcentaje de Reportes entregados en el plazo establecido antes y después de implementado el sistema web.

		N	Rango promedio	Suma de rangos
% Reportes entregados en el plazo establecido - POSTEST - % Reportes entregados en el plazo establecido- PRETEST	Rangos negativos	0[a]	,00	,00
	Rangos positivos	24[b]	12,50	300,00
	Empates	6[c]		
	Total	30		

a. % Reportes entregados en el plazo establecido- POSTEST < % Reportes entregados en el plazo establecido - PRETEST

b. % Reportes entregados en el plazo establecido - POSTEST > % Reportes entregados en el plazo establecido - PRETEST

c. % Reportes entregados en el plazo establecido - POSTEST = % Reportes entregados en el plazo establecido - PRETEST

De los resultados obtenidos de la tabla 9 podemos ver que la variable PREPEa es menor que la variable PREPEd por lo tanto la Hipótesis Nula es rechazada y se acepta la Hipótesis Alterna.

B. Hipótesis de investigación 2

H2: El Sistema web mejora significativamente la integridad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos. – La Molina

Indicador: Porcentaje de Reportes Íntegros generados

Hipótesis Estadística

Definición de Variables:

PRIGa: Porcentaje de Reportes Íntegros generados antes de implementar el sistema web.

PRIGd: Porcentaje de Reportes Íntegros generados después de implementar el sistema web.

H2o: El uso del sistema web no aumenta el porcentaje de Reportes Íntegros generados.

$$H2o: PRIGd \leq PRIGa$$

H2a: El uso del sistema web aumenta el porcentaje de Reportes Íntegros generados.

$$H2a: PRIGd > PRIGa$$

Tabla 10. Diferencia significativa en el Porcentaje de Reportes Íntegros generados antes y después de implementado el sistema web.

	Z	Sig. asintótica (bilateral)
% Reportes Íntegros generados - POSTEST - % Reportes Íntegros generados - PRETEST	-4,289[b]	,000

a. Prueba de Wilcoxon de los rangos con signo

b. Se basa en rangos negativos.

Los resultados de la prueba de Wilcoxon muestran que el P valor es de 0.000 menor a 0.05 lo que significa que existe diferencia significativa en el Porcentaje de Reportes Íntegros generados antes y después de implementado el sistema web.

Tabla 11. Rangos de Porcentaje de Reportes Íntegros generados antes y después de implementado el sistema informático.

		N	Rango promedio	Suma de rangos
% Reportes Íntegros generados - POSTEST - % Reportes Íntegros generados - PRETEST	Rangos negativos	1[a]	1,00	1,00
	Rangos positivos	23[b]	13,00	299,00
	Empates	6[c]		
	Total	30		

a. % Reportes Íntegros generados - POSTEST < % Reportes Íntegros generados - PRETEST

b. % Reportes Íntegros generados - POSTEST > % Reportes Íntegros generados - PRETEST

c. % Reportes Íntegros generados - POSTEST = % Reportes Íntegros generados - PRETEST

De los resultados obtenidos de la tabla 11 podemos ver que la variable PRIGa es menor que la variable PRIGd por lo tanto la Hipótesis nula es rechazada y se acepta la Hipótesis alterna.

C. Hipótesis de investigación 3

H2: El Sistema web mejora significativamente la confidencialidad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos. – La Molina

Indicador: Porcentaje Reportes Confidenciales Entregados Correctamente

Hipótesis Estadística

Definición de Variables:

PRCECa: Porcentaje Reportes Confidenciales Entregados Correctamente antes de implementar el sistema web.

PRCECd: Porcentaje Reportes Confidenciales Entregados Correctamente después de implementar el sistema web.

H2o: El uso del sistema web no aumenta el Porcentaje Reportes Confidenciales Entregados Correctamente

$$H2o: PRCECd \leq PRCECa$$

H2a: El uso del sistema web aumenta el Porcentaje Reportes Confidenciales Entregados Correctamente.

$$H2a: PRCECd > PRCECa$$

Tabla 12. Diferencia significativa en el Porcentaje Reportes Confidenciales Entregados Correctamente antes y después de implementado el sistema web.

	Z	Sig. asintótica (bilateral)
% Reportes Confidenciales Entregados Correctamente - POSTEST - % Reportes Confidenciales Entregados Correctamente - PRETEST	-3,543[b]	,000

a. Prueba de Wilcoxon de los rangos con signo

b. Se basa en rangos negativos.

Los resultados de la prueba de Wilcoxon muestran que el P valor es de 0.000 menor a 0.05 lo que significa que existe diferencia significativa en el Porcentaje Reportes Confidenciales Entregados Correctamente antes y después de implementado el sistema web.

Tabla 13. Rangos de Porcentaje Reportes Confidenciales Entregados Correctamente antes y después de implementado el sistema web.

		N	Rango promedio	Suma de rangos
% Reportes Confidenciales Entregados Correctamente - POSTEST - % Reportes Confidenciales Entregados Correctamente - PRETEST	Rangos negativos	3[a]	4,67	14,00
	Rangos positivos	18[b]	12,06	217,00
	Empates	9[c]		
	Total	30		

a. % Reportes Confidenciales Entregados Correctamente - POSTEST < % Reportes Confidenciales Entregados Correctamente - PRETEST

b. % Reportes Confidenciales Entregados Correctamente - POSTEST > % Reportes Confidenciales Entregados Correctamente - PRETEST

c. % Reportes Confidenciales Entregados Correctamente - POSTEST = % Reportes Confidenciales Entregados Correctamente - PRETEST

De los resultados obtenidos de la tabla 13 podemos ver que la variable PRCECd es mayor que la variable PRCECa por lo tanto la Hipótesis nula es rechazada y se acepta la Hipótesis alterna.

IV. DISCUSIÓN

Con los resultados obtenidos en la presente investigación se analizó y se comparó el "Porcentaje de Reportes entregados en el plazo establecido", "Porcentaje de Reportes Íntegros generados" y el "Porcentaje de Reportes Confidenciales Entregados Correctamente", antes y después de la implementación del Sistema web para la gestión de la seguridad de la información en la empresa de Servicios Informáticos S.A.C.

Estos resultados se pueden contrastar con la investigación de Ramírez (2017), quien a través de la implementación de un sistema web pudo obtener una mejora significativa respecto a los procesos de gestión. Asimismo se tiene la investigación que ha sido realizada por Justino (2015), quien también diseño un sistema Web logrando un mejor control de su gestión de seguridad.

1-El Porcentaje de Reportes entregados en el plazo establecido, en la medición pretest, la media alcanzó 72.33 % y con la implementación del sistema web la media aumentó a 97.94%. Los resultados obtenidos indican que existe una diferencia positiva de 25.61%, por lo que se puede confirmar que con la implementación del sistema web se ha logrado aumentar el Porcentaje de Reportes entregados en el plazo establecido al área de backup de la empresa de Servicios Informáticos S.A.C.

Estos resultados se pueden comparar con los obtenidos con Guillermo (2017), quien también implemento un sistema Web con la cual logró mayor eficacia de los trabajadores, por lo que no existen tiempos muertos, pues se ha aplicado modos de marcación, demostrándose la probabilidad de conseguir contactabilidad y el posterior cierre de venta.

2-El Porcentaje de Reportes Íntegros generados, en la medición pretest, la media alcanzó 74.06 % y con la implementación del sistema web la media disminuyó a 97.94 %. Los resultados obtenidos indican que existe una diferencia positiva de 23.88 %, por lo que se puede confirmar que con la implementación del sistema web se ha logrado aumentar el Porcentaje de Reportes Íntegros generados al área de backup de la empresa de Servicios Informáticos S.A.C.

En la cual se toma como referencia la investigación de Urrego y Soto (2015), con respecto a los reportes íntegros manifiestan que los sistemas de información web presentan gran funcionalidad en el contexto organizacional de cualquier empresa, porque ayuda a un mejor procesamiento de estos datos.

3-El Porcentaje de Reportes Confidenciales Entregados Correctamente, en la medición pretest, la media alcanzó 77.39 % y con la implementación del sistema web la media disminuyó a 96.67 %. Los resultados obtenidos indican que existe una diferencia positiva de 19.28 %, por lo que se puede confirmar que con la implementación del sistema web se ha logrado aumentar el Porcentaje de Reportes Confidenciales Entregados Correctamente al área de backup de la empresa de Servicios Informáticos S.A.C.

Para lo cual se tomará como referencia la investigación de Ríos (2018) con respecto a los reportes confidenciales, pudo evidenciar que el sistema web contribuye a centralizar la información de sus diferentes puntos de ventas, de manera que la información que se tiene de los reportes confidenciales se realizan de manera eficiente, organizándose de forma idónea.

V. CONCLUSIONES

Las apreciaciones finales son:

1. Se ha comprobado que el Porcentaje de Reportes entregados en el plazo establecido, utilizando el sistema web en la gestión de la seguridad de la información de la empresa Servicios Informáticos S.A.C. aumentó, sin el sistema web la media fue de 72.33% y con uso del sistema web la media fue de 97.94, logrando un aumento de 25.61%.

2. Se ha comprobado que el Porcentaje de Reportes Íntegros generados haciendo uso de un software web en la administración en seguridad de la información en la empresa Servicios Informáticos S.A.C. aumento, sin el sotfware web la media fue 74.06 % , pero con uso del software web la media fue 97.94 %, logrando un aumento de 23.88%

2. Se ha determinado que el Porcentaje de Reportes Confidenciales Entregados Correctamente utilizando el sistema web en la gestión de la seguridad de la información de la empresa Servicios Informáticos S.A.C. aumento, sin el sistema web la media fue de 77.39 % y con uso del sistema web la media fue de 96.67 %, logrando un aumento de 19.28%

VI. RECOMENDACIONES

Mis recomendaciones para futuros trabajos de tesis son1:

1. Se sugiere de ser posible tomar como muestra a toda la población para tener resultados más precisos.

2. Finalmente, para obtener resultados estadísticos más precisos se puede considerar ampliar el periodo de pruebas.

VII. REFERENCIAS.

Aliaga, L. (2013). *"Diseño de un sistema de gestión de seguridad de información para un instituto educativo"*. Tesis para optar el título de Ingeniero Informático, que presenta el bachiller de la Pontificia Universidad Católica del Perú, Lima. Perú.

Alcántara, J. (2015).*"Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo"*. Tesis para optar el título de ingeniero de Sistemas y Computación de la Universidad Católica Santo Toribio de Mogrovejo, Chiclayo. Perú.

Aguirre, J. y Aristizabal, C. (2013). *Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la OFRENDA*. (Tesis de grado) Universidad Tecnológica de Pereira, Colombia.

Alexander, G. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información*. Primera edición. Colombia: Alfaomega

Areitio, J. (2008). *Seguridad de la Información: redes, informática y sistemas de información*. España: Learning Paraninfo S.A.

Arisaca, F. y Quispe, S. (2016). *Desarrollo de una propuesta de implementación de la NTPISO/IEC 27001:2014, sistema de gestión de seguridad de la información, para la oficina funcional de informática del gobierno regional del Cusco*. (Tesis para optar el título de ingeniero informático de sistemas). Universidad Nacional de San Antonio ABAD del Cusco, Cusco.

Arque (2017). *Implementación de un sistema de gestión en seguridad y salud ocupacional en el rubro de construcción de PAD de Lixiviación en la empresa AJANI SAC*. (Tesis de grado). Universidad Nacional del Altiplano, Puno, Perú.

Baez, S. (2012). *Sistema web*, Recuperado de http://www.knowdo.org/knowledge/39-sistemas-web, Fecha de acceso 16/04/14.

Barrantes, C. y Hugo, J. (2012). *Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos*. (Tesis de grado) Universidad San Martín de Porras, Lima – Perú.

Berrio, J. (2016). Metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad de información sobre la norma ISO/IEC 27001. (Tesis de maestría). Universidad Nacional de Colombia, Colombia.

Bermúdez, K. y Bailón, E. (2015). Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001 – sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros. (Tesis de grado). Universidad

Politécnica Salesiana, Guayaquil, Ecuador.

Berrospi, R. y Pilar, J. (2017). *Implementación de un sistema web para optimizar la gestión académica en la I.E. "Villa Corazón de Jesús" del Distrito de San Juan de Lurigancho, 2013.* (Tesis para optar el título profesional de ingeniero de sistemas e informática). Universidad de Ciencias y Humanidades, Lima.

Callán, H. Ramos, V. y Solano, R. (2017). Implementación de un Sistema Web para el Control y Monitoreo de la Empresa AB Seguridad E.I.R.L. (Tesis para optar el título de ingeniero en computación y sistemas). Universidad Peruanas de las Américas, Lima.

Carolina, A. (2017). Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013". (Tesis de grado). Institución Universitaria Politécnico Grancolombiano, Colombia.

Castillo, A. (2018). *Implementación de un sistema web de compra y venta para la distribuidora Salas - Huarmey; 2017*. (Tesis para optar el título profesional de ingeniero de sistemas). Universidad Católica Los Ángeles Chimbote; Chimbote.

Chapin, A. y Akridge, S. (2005) *¿Cómo Puede Medirse la Seguridad?* Disponible en: http://www.iso27000.es/download/HowCanSecurityBeMeasured-SP.pdf. Consultado Diciembre 9, 2011.

Cohen, D. (1996). *Sistemas de Información para los negocios. Un enfoque para la toma de decisiones*, McGraw-Hill/Interamericana Editores S.A. México, 3ra Edición.

Ccesa, M. (2017). Diseño de un sistema de gestión de seguridad de la información bajo la NTP ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016. (Tesis para optar el título de ingeniero informático). Universidad Nacional de San Cristóbal de Huamanga, Ayacucho.

Cupitán, J. (2017). *"Diseño e implementación de una aplicación web de venta online para la empresa grupo Company S.A.C., Chimbote; 2015"*. Tesis para optar el título de ingeniero de Sistemas de la Universidad Católica los Ángeles, Chimbote. Perú.

Diario Gestión. (2010). *Tarjetas de crédito acelerarían crecimiento en último trimestre*. Disponible en: http://gestion.pe/noticia/667537/tarjetascredito-acelerarian-crecimiento-ultimo-trimestre. Consultado Diciembre 10, 2011

Díaz, A. (2010). *Sistema de Gestión de la Seguridad de la Información UNE-ISO/IEC 27001* (En línea). (Consultado el 17 de mayo del 2018). Recuperado en: https://www.aec.es/c/document_library/get_file?p_l_id=239310&folderId=195657&name=DLFE-7132.pdf

Espinoza, H. (2013). *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo*. Pontificia Universidad Católica del Perú.

Fernández, D. y Pacheco, O. (2014). Mejora de seguridad de información en la comandancia de operaciones guardacostas basada en la norma técnica peruana NTP-ISO/IEC 27001:2008. (Tesis para optar el grado de ingeniero de computación y sistemas) Universidad San Martín de Porras, Lima.

Flores, C. (2017). *Diseño del sistema de gestión de seguridad de la información para el Grupo SIAS SAC. – Chimbote; 2017*. (Tesis para optar el título profesional de Ingeniero de Sistemas). Universidad Católica Los Ángeles de Chimbote, Chimbote.

Frayssinet, M. (2014). *Taller de transición de la norma ISO/IEC 27001:2005 a la ISO/IEC 27001:2013*. Oficina Nacional de Gobierno Electrónico e Informática - OGEI. Lima.

Guillermo, R. (2017). Implementación de un sistema Web para las ventas en la empresa One To One Contact Solutions. (Tesis para optar el grado de ingeniero empresarial y de sistemas). Universidad San Ignacio de Loyola, Lima.

Gómez, E. (2017). "*Implementación de un sistema de información bajo plataforma web para la gestión y control documental de la empresa Corporación Jujedu E.I.R.L. – talara; 2017*". Tesis de Licenciatura. Universidad de Católica los Ángeles de Chimbote.

Grupo ACMS Consultores (2017). *UNE-ISO/IEC 27001- Protección ante Riesgos de la Seguridad de la Información.* (En línea). (Consultado el 18 de mayo del 2018). Recuperado en: https://www.grupoacms.com/blog/une-isoiec-27001-proteccion-riesgos-seguridad-informacion/

Guamán, J. (2015). *Diseño de un sistema de gestión de seguridad de la información para Instituciones Militares*. (Tesis de maestría). Escuela Politécnica Nacional, Ecuador.

Guerrero, Y. y Tabango, R. (2014). *Sistema de gestión de seguridad de la información (SGSI) basada en la Norma ISO 27001 y 27002 para la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño*. (Tesis de grado) Universidad de Nariño, Colombia.

Guzmán, A y Taborda, C. (2015). Diseño de un sistema de gestión de la seguridad informática -SGSI- para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C. a través de la auditoria. (Tesis para optar el grado de especialista en seguridad informática). Universidad Nacional Abierta y a Distancia, Bogotá, Colombia.

Guzmán, C. (2015). Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso. (Tesis de grado). Institución Universitaria Politécnico Grancolombiano, Colombia.

Guerrón, J. (2013). *"Elaboración de un plan para la implementación del sistema de gestión de seguridad de la información"*. Trabajo de Fin del Máster Interuniversitario en Seguridad de las Tecnologías de la Información y las Comunicaciones de la Universidad Abierta de Cataluña, España.

Hernández, R., Fernández, C. y Baptista, M. P. (2014). *Metodología de la investigación*. McGRAW-HILL / Interamericana Editores, S.A. DE C.V. México.

Hernández, R., Fernández, C. y Baptista, P. (2006). *Metodología de la investigación*, C4ta versión, McGraw-Hill interamericana.

Ibujés, L. (2017). *Diseño del Sistema Web de Administración de Proyectos Tecnológicos para Organizaciones*. Universidad Internacional de la Rioja. Quito. Colombia.

Instituto Nacional de Estadística y Geografía (2017), *Políticas para la seguridad de la información del Instituto Nacional de Estadística y Geografía*. México.

ISACA (2012a). "*Governance of Enterprise IT (GEIT) Survey"* Global Edition, ISACA. Consulta: 25 de Abril de 2013: http://www.isaca.org/GEITSurvey2012

ISO/IEC 27001:2005. (2005). *Estándar Internacional. Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de Seguridad de la Información – Requerimientos*

Justino (2015). *Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la Norma ISO / IEC 27001:2013*. (Tesis de grado). Universidad Católica del Perú, Lima, Perú.

Laudon, K. y Laudon, J. (2012). *Sistemas de información gerencial*. Duodécima edición. México: Pearson Educación.

López A, Ruiz J. (2005). *MODELO ISO 27000*. Disponible en: "http://www.iso27000.es/" http://www.iso27000.es/

Maureira, D. (2017). Norma ISO/IEC 27001 aplicada a una carrera universitaria. (Tesis de grado). Universidad Andrés Bello, Chile.

Mesquida, A., Alcover, A. y Mas, A. (2010). *Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001*. Revista Española de Innovación, Calidad e Ingeniería del Software Volumen 6, Número 3 (especial XI JICS), noviembre.

Molina, A. (2015). Definición y validación de procesos de gestión de seguridad de la información para la empresa Amisoft. (Tesis de maestría). Tecnologías de la información de la Universidad de Chile, Chile.

Morán, J. (2016). Desarrollo de un sistema web para el control administrativo de los equipos camineros del Gad Municipal de Pedro Carbo. (tesis para optar el título profesional de ingeniero en sistemas computacionales). Universidad de Guayaquil-Ecuador.

Moyano, L. y Suárez, Y. (2017). *Plan de implementación del SGSI basado en la norma ISO 27001:2013 para la empresa interfaces y soluciones*. Tesis de grado de la Universidad Distrital Francisco José de Caldas, Bogotá.

Ñaupas, H., Mejía, E., Novoa, E. & Villagómez, A. (2013). *Metodología de la investigación científica y elaboración de tesis*. 3º edición. Perú. Editorial e imprenta Universidad Nacional Mayor de San Marcos.

Ochoa, A. (2017). *Sistema web de gestión de seguridad de la información asistida por computadora basada en el estándar ISO 27001 en la Universidad Nacional José María Arguedas*. (Tesis para optar el título profesional de ingeniero de sistemas). Universidad Nacional José María Arguedas, Apurímac.

Ortiz, C. y Martínez, C. (2016). *Mejores prácticas en la Implantación de ISO27001:2013 y PCI/DSS 3.1*. (Tesis para optar el título de ingeniero técnico en informática y gestión). Universidad Abierta de Cataluña, España.

Pinto, J. (2017). *Gestión y riesgos de seguridad de la información en la Escuela de Suboficiales de la Policía Nacional del Perú, Puente Piedra 2016*. (Tesis de maestría). Universidad Nacional de Educación Enrique Guzmán y Valle, Lima.

Quispe, A. y Vargas, F. (2016). Implementación de un sistema de información web para optimizar la gestión administrativa de la Empresa Comercial Angelito de la Ciudad de Chepén. (Tesis para optar el título de ingeniero de sistemas). Universidad Nacional de Trujillo, Trujillo.

Ramírez, J. (2017). *Implementación de un sistema web para mejorar el proceso de gestión académica en las escuelas de la PNP*. (Tesis de Licenciatura). Universidad Peruana de las Américas. Lima. Perú.

Ramos, A. (2011*). Aplicaciones web: Sistemas microinformáticos y redes* .ed. Paraninfo, .p 17. ISBN 8497328132,

Rios, J. (2014). *Diseño de un sistema de gestión de seguridad de información para una central privada de información de riesgos*. (Tesis de grado) Pontificia Universidad Católica del Perú, Lima – Perú.

Ríos, F. (2018). Sistema web para mejorar el control de inventarios en la empresa Comercial Lucerito, 2018. (Tesis para optar el grado de ingeniero de sistemas e información). Universidad Norbert Wiener, Lima.

Rivera, M. (2017). *Gestión municipal de transporte Urbano y la satisfacción del usuario en Lima Cercado en el año 2016*. (Tesis de maestría). Universidad César Vallejo, Sede Lima

Salcedo, R. (2014). *Plan de implementación del SGSI basado en la norma ISO 27001:2013*. Tesis de grado de la Universidad Abierta de Cataluña, España.

Santos, D. (2016). *Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software*. (Tesis para optar por el Título de Ingeniero Informático,). Pontificia Universidad Católica del Perú, Lima.

Suárez, S. (2015): Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez Padilla & Cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización.". (Tesis para optar el grado de especialista en seguridad informática). Universidad Nacional Abierta y a Distancia, Bogotá, Colombia

Suca, J. (2014). Propuesta metodológica para implementar la Norma Técnica Peruana ISO/IEC 27001:2008 de Seguridad de la Información en entidades públicas del Estado. (Tesis para optar el título de ingeniero de sistemas). Universidad Católica de Santa María, Arequipa.

Tacuri, H. (2015). *Sistema web de gráficos en el control de salud epidemiológico del Minsa Sandia – 2015*. (Tesis para título profesional de: ingeniero estadístico e informático). Universidad Nacional del Altiplano – Puno.

Talavera, V. (2015). *Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISI/IEC 27001:2013*. (Tesis para optar por el Título de Ingeniero Informático). Pontificia Universidad Católica del Perú, Lima.

Tarrillo, E. y Correa, J. (2015). *Metodología para un sistema de gestión de la seguridad de la información basado en la Norma Técnica Peruana NTP- 17799 en la administración de la Municipalidad Distrital de Lambayeque setiembre 2013 - febrero 2014.* (Tesis para optar el título profesional de ingeniero de sistemas). Universidad Nacional Pedro Ruiz Gallo, Lambayeque.

TÜV SÜD (2013). ISO/IEC 27001 *Gestión de seguridad de la información*. (En línea). (Consultado el 18 de mayo del 2018). Recuperado en: http://www.tuv-sud.es/uploads/images/1381756891144339900235/es-tuv-sud-iso-iec-27001-sistema-gestion-seguridad-

informacion.pdf

Tola, D. (2015). Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001 (tesis de licenciatura). Escuela Superior Politécnica del Litoral. Guayaquil-Ecuador.

Van, D. y Meyer, W. (2006). *Manual de técnica de la Investigación educacional*.

Vara, A. (2012) *Siete pasos para una tesis exitosa. Un método efectivo para las ciencias empresariales. Instituto de investigación de la facultad de ciencias administrativas y recursos humanos*. Universidad de San Martin de Porres. Lima. Manuel electrónico disponible en internet: www.aristidesvara.net, pág. 221, 223.

Vargas, J. (2017). Sistema web para el proceso de venta en la empresa Calzatec E.I.R.L. (Tesis para optar el grado de ingeniero de sistemas). Universidad César Vallejo, Lima.

Vilca, E. (2017). Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa Geosurvey de la ciudad de Lima. (Tesis para optar el grado de ingeniero de sistemas e informática). Universidad de Huánuco.

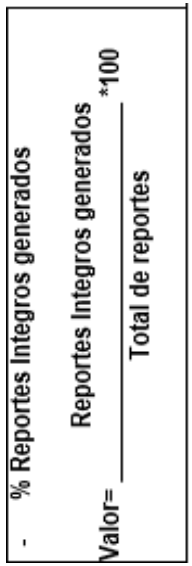
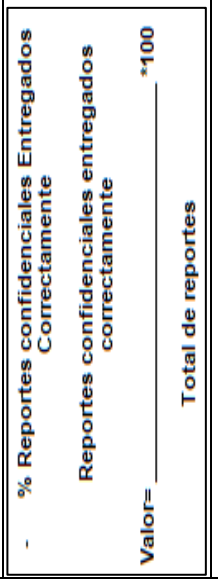
Urrego, R. Soto, C. (2015) en su trabajo de investigación "Sistema de información web para agilizar el proceso de radicación y registro de actividades en el área tecnológica para pequeñas empresas (SIPRA)"; (Tesis para optar el título profesional de tecnólogo en sistematización de datos). Universidad Distrital Francisco José de Caldas, *Colombia*.

Zeña, V. (2015). *Estándar internacional iso 27001 para la gestión de seguridad de la información en la Oficina Central de Informática de la UNPRG*. (Tesis para optar el Título de Ingeniero de Sistemas). Universidad Nacional Pedro Ruiz Gallo, Lambayeque.

ANEXOS

ANEXO 1: Matriz de consistencia

TITULO GENERAL	PREGUNTA DE INVESTIGACIÓN	OBJETIVOS	HIPÓTESIS	VARIABLE	DEFINICION CONCEPTUAL		DEFINICIÓN OPERACIONAL			ESCALA
	PROBLEMA GENERAL	OBJETIVO GENERAL	HIPÓTESIS GENERAL	INDEPENDIENTE						
SISTEMA WEB PARA LA GESTION DE LA SEGURIDAD DE LA INFORMACION ALINEADA A LA NORMA ISO/IEC 27001 EN UNA EMPRESA DE SERVICIOS INFORMATICOS	¿Cuál será el efecto de un Sistema web en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos - La Molina?	Determinar el efecto de un Sistema web en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informático - La Molina	El sistema web aumenta significativamente en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informático - La Molina.	Sistema Web	En este sentido Ramos (2011) define un sistema web como un recurso de información o un proceso de negocio, al que se puede acceder otra aplicación a través de la web y con el cual se puede comunicar a través de protocolos estándares de internet.		. La particularidad que tienen los sistemas web es que están diseñados para permitir la comunicación de una aplicación con otra, sin intervención humana. Por su parte Baez (2012) señala que el sistema web o también conocido como aplicación web es aquella que está desarrollada e instalada no sobre una plataforma o un sistema operativo (Windows, Linux), los cuales se hallan en servidores de internet o sobre una intranet (red local)			
	PROBLEMAS ESPECÍFICOS	**OBJETIVOS ESPECÍFICOS**	**HIPÓTESIS ESPECÍFICOS**	**DEPENDIENTE**	**DEFINICIÓN CONCEPTUAL**	**DEFINICIÓN OPERACIONAL**	**DIMENSIONES**	**NDICADOR**	**FÓRMULA**	
	¿Cuál será el efecto de un Sistema web en la disponibilidad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos - La Molina?	Analizar el efecto de un Sistema web en la disponibilidad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la Empresa de Servicios Informáticos - La Molina	El Sistema web mejora significativamente la disponibilidad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos - La Molina	Gestión de la seguridad de la información	Según Terry (citado en Rivera, 2017) se define la gestión como un proceso que consiste en la planificación, organización, accionar y controlar, realizado para determinar y llevar a cabo los objetivos mediante el uso de personas y recursos.	La seguridad de la información en las empresas hoy en día es de suma responsabilidades, procesos, procedimientos y recursos que establece la alta dirección con el propósito de dirigir y controlar la seguridad de los activos de información y asegurar la continuidad de la operatividad de la empresa.se evalúa a través de sus dimensiones en un cuestionario	Disponibilidad de la información	% Reportes entregados en el plazo establecido	$\text{Valor} = \frac{\text{\% Reportes entregados en el plazo establecido}}{\text{Reportes entregados en el plazo establecido}} * 100$ Total de reportes	Razón

	¿Cuál será el efecto de un Sistema web en la integridad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos - La Molina?	Identificar el efecto de un Sistema web en la integridad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos - La Molina	El Sistema web mejora significativamente la integridad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos - La Molina				Integridad de la información	% Reportes Íntegros generados	
	¿Cuál será el efecto de un Sistema web en la confidencialidad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos . La Molina?	Identificar el efecto de un Sistema web en la confidencialidad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos - La Molina	El Sistema web mejora significativamente la confidencialidad en la gestión de la seguridad de la información alineado a la norma ISO/IEC 27001 en la empresa de servicios informáticos - La Molina				Confidencialidad de la información	% Reportes Confidenciales entregados correctamente	

Anexo 2: Ficha de Observación

FICHA DE OBSERVACION	
Observador:	José Miguel Aguirre Ventura
Institución donde se investiga:	Empresas de Servicios Informáticos S.A.C
Ubicación de la institución:	Avenida Javier Prado Este 6230 - La Molina
Indicador utilizado:	Porcentaje de Reportes entregados en el plazo establecido
Periodo de la observación Pretest:	01/08/2018 - 31/08/2018
Periodo de la observación Postest:	01/09/2018 - 30/09/2018

	PRETEST: Agosto 2018			POSTEST: Septiembre 2018		
Informes diarios	**Reportes entregados en el plazo establecido**	**Total de reportes**	**Resultado %**	**Reportes Entregados en el plazo establecido**	**Total de reportes**	**Resultado %**
1	2	4	50,00	5	5	100,00
2	2	5	40,00	4	4	100,00
3	3	6	50,00	3	4	75,00
4	4	6	66,67	5	5	100,00
5	3	5	60,00	4	4	100,00
6	4	4	100,00	6	6	100,00
7	3	5	60,00	4	5	80,00
8	4	6	66,67	5	5	100,00
9	3	5	60,00	4	4	100,00
10	3	5	60,00	5	6	83,33
11	4	5	80,00	4	4	100,00
12	4	6	66,67	5	5	100,00
13	3	3	100,00	4	4	100,00
14	4	6	66,67	5	5	100,00
15	3	5	60,00	5	5	100,00
16	3	4	75,00	6	6	100,00
17	4	5	80,00	4	4	100,00
18	2	4	50,00	6	6	100,00
19	3	5	60,00	5	5	100,00
20	3	4	75,00	3	3	100,00
21	4	5	80,00	5	5	100,00
22	5	5	100,00	6	6	100,00
23	4	6	66,67	4	4	100,00
24	4	5	80,00	3	3	100,00
25	3	4	75,00	6	6	100,00
26	4	6	66,67	3	3	100,00
27	3	3	100,00	6	6	100,00
28	3	4	75,00	4	4	100,00
29	3	3	100,00	4	4	100,00
30	4	4	100,00	5	5	100,00

Promedio:	**3,37**	**4,77**	**72,33**	**4,60**	**4,70**	**97,94**

FICHA DE OBSERVACION	
Observador:	Josè Miguel Aguirre Ventura
Institución donde se investiga:	Empresas de Servicios Informaticos S.A.C
Ubicación de la institución:	Avenida Javier Prado Este 6230 - La Molina
Indicador utilizado:	Porcentaje de Reportes Íntegros generados
Periodo de la observación Pretest:	01/08/2018 - 31/08/2018
Periodo de la observación Postest:	01/09/2018 - 30/09/2018

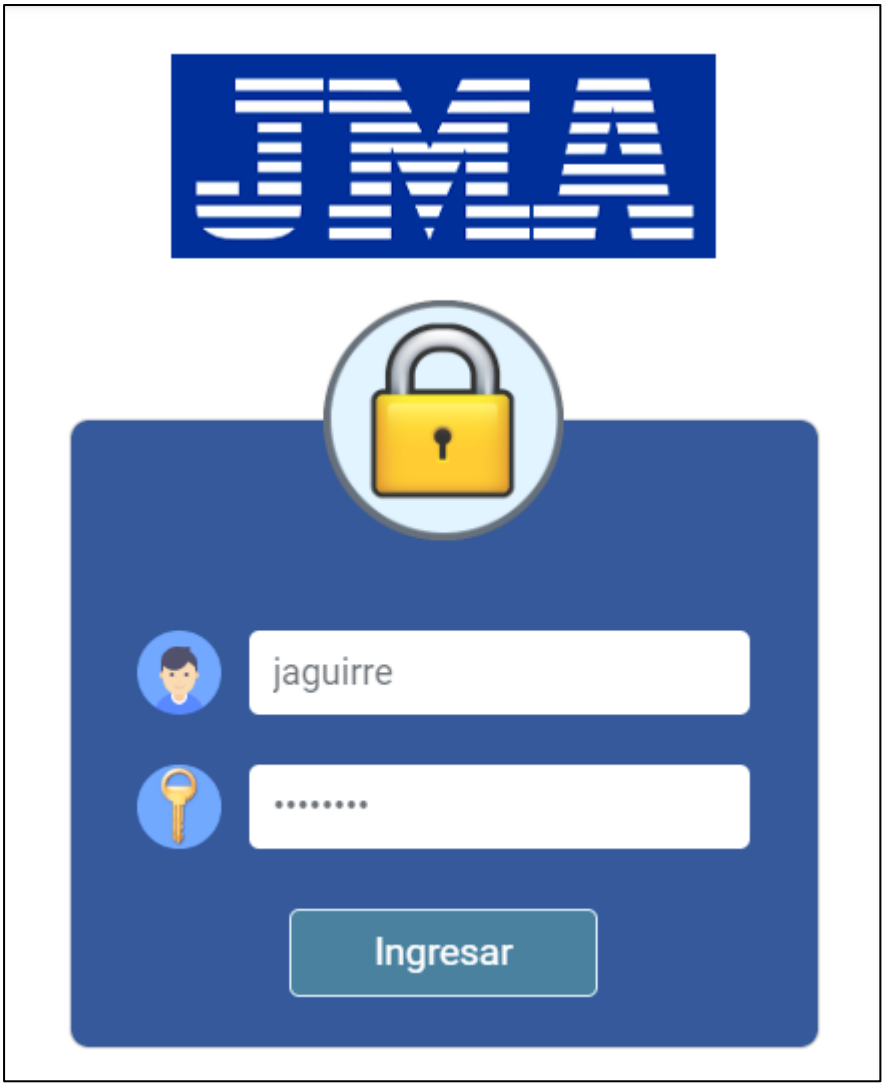
	PRETEST: Agosto 2018			**POSTEST: Septiembre 2018**		
Informes diarios	**Reportes Íntegros generados**	**Total de reportes**	**Resultado %**	**Reportes Íntegros generados**	**Total de reportes**	**Resultado %**
1	2	4	50,00	4	4	100,00
2	4	5	80,00	3	4	75,00
3	3	6	50,00	4	4	100,00
4	3	6	50,00	5	5	100,00
5	4	5	80,00	4	4	100,00
6	3	4	75,00	6	6	100,00
7	4	5	80,00	4	4	100,00
8	3	6	50,00	3	3	100,00
9	3	4	75,00	4	4	100,00
10	5	5	100,00	6	6	100,00
11	4	5	80,00	4	5	80,00
12	4	6	66,67	5	5	100,00
13	3	4	75,00	5	6	83,33
14	4	5	80,00	5	5	100,00
15	4	5	80,00	5	5	100,00
16	3	4	75,00	3	3	100,00
17	4	5	80,00	6	6	100,00
18	2	4	50,00	4	4	100,00
19	3	5	60,00	5	5	100,00
20	3	4	75,00	4	4	100,00
21	4	5	80,00	5	5	100,00
22	5	5	100,00	6	6	100,00
23	3	4	75,00	4	4	100,00
24	4	5	80,00	4	4	100,00
25	3	4	75,00	5	5	100,00
26	3	6	50,00	3	3	100,00
27	3	3	100,00	6	6	100,00
28	2	4	50,00	5	5	100,00
29	3	3	100,00	4	4	100,00
30	4	4	100,00	5	5	100,00
Promedio:	**3,40**	**4,67**	**74,06**	**4,53**	**4,63**	**97,94**

FICHA DE OBSERVACION	
Observador:	José Miguel Aguirre Ventura
Institución donde se investiga:	Empresas de Servicios Informáticos S.A.C
Ubicación de la institución:	Avenida Javier Prado Este 6230 - La Molina
Indicador utilizado:	Porcentaje de Reportes Confidenciales Entregados Correctamente
Periodo de la observación Pretest:	01/08/2018 - 31/08/2018
Periodo de la observación Postest:	01/09/2018 - 30/09/2018

	PRETEST: Agosto 2018			POSTEST: Septiembre 2018		
Informes diarios	**Reportes Confidenciales Entregados Correctamente**	**Total de reportes**	**Resultado %**	**Reportes Confidenciales Entregados Correctamente**	**Total de reportes**	**Resultado %**
1	2	2	100,00	2	3	66,67
2	3	3	100,00	4	4	100,00
3	1	2	50,00	4	4	100,00
4	4	4	100,00	5	5	100,00
5	3	3	100,00	4	4	100,00
6	3	3	100,00	6	6	100,00
7	3	5	60,00	4	4	100,00
8	3	3	100,00	3	3	100,00
9	3	3	100,00	4	4	100,00
10	3	5	60,00	5	6	83,33
11	2	4	50,00	5	6	83,33
12	3	5	60,00	5	5	100,00
13	3	3	100,00	5	6	83,33
14	3	4	75,00	5	5	100,00
15	2	4	50,00	5	5	100,00
16	3	3	100,00	3	3	100,00
17	2	4	50,00	6	6	100,00
18	2	2	100,00	4	4	100,00
19	2	3	66,67	5	5	100,00
20	3	4	75,00	4	4	100,00
21	3	5	60,00	5	5	100,00
22	4	5	80,00	6	6	100,00
23	3	4	75,00	4	4	100,00
24	3	5	60,00	4	4	100,00
25	3	4	75,00	5	5	100,00
26	3	6	50,00	3	3	100,00
27	3	3	100,00	5	6	83,33
28	2	4	50,00	5	5	100,00
29	3	3	100,00	4	4	100,00
30	3	4	75,00	5	5	100,00
Promedio:	**2,77**	**3,73**	**77,39**	**4,47**	**4,63**	**96,67**

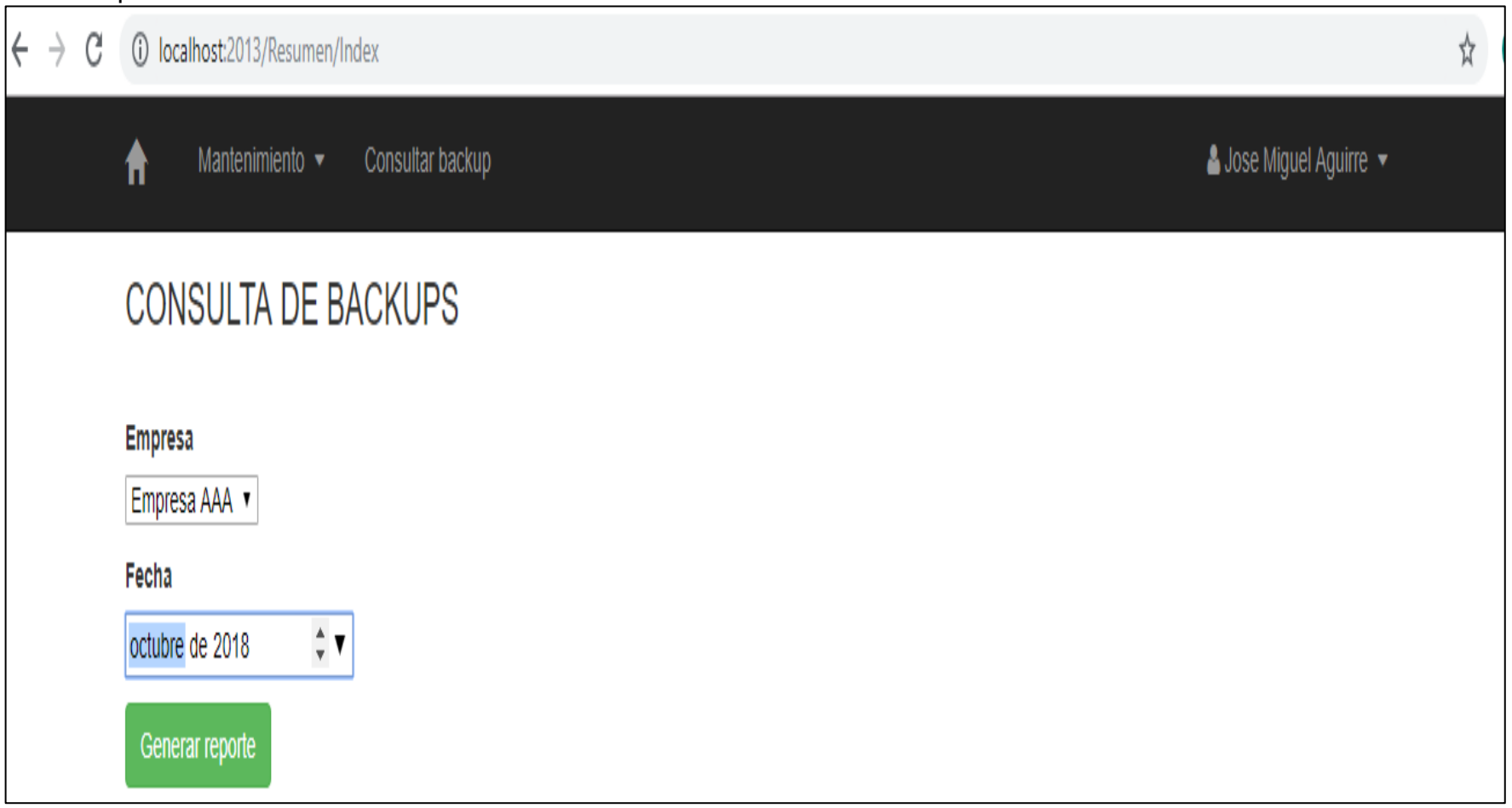
Anexo 3: Sistema Web

Login:



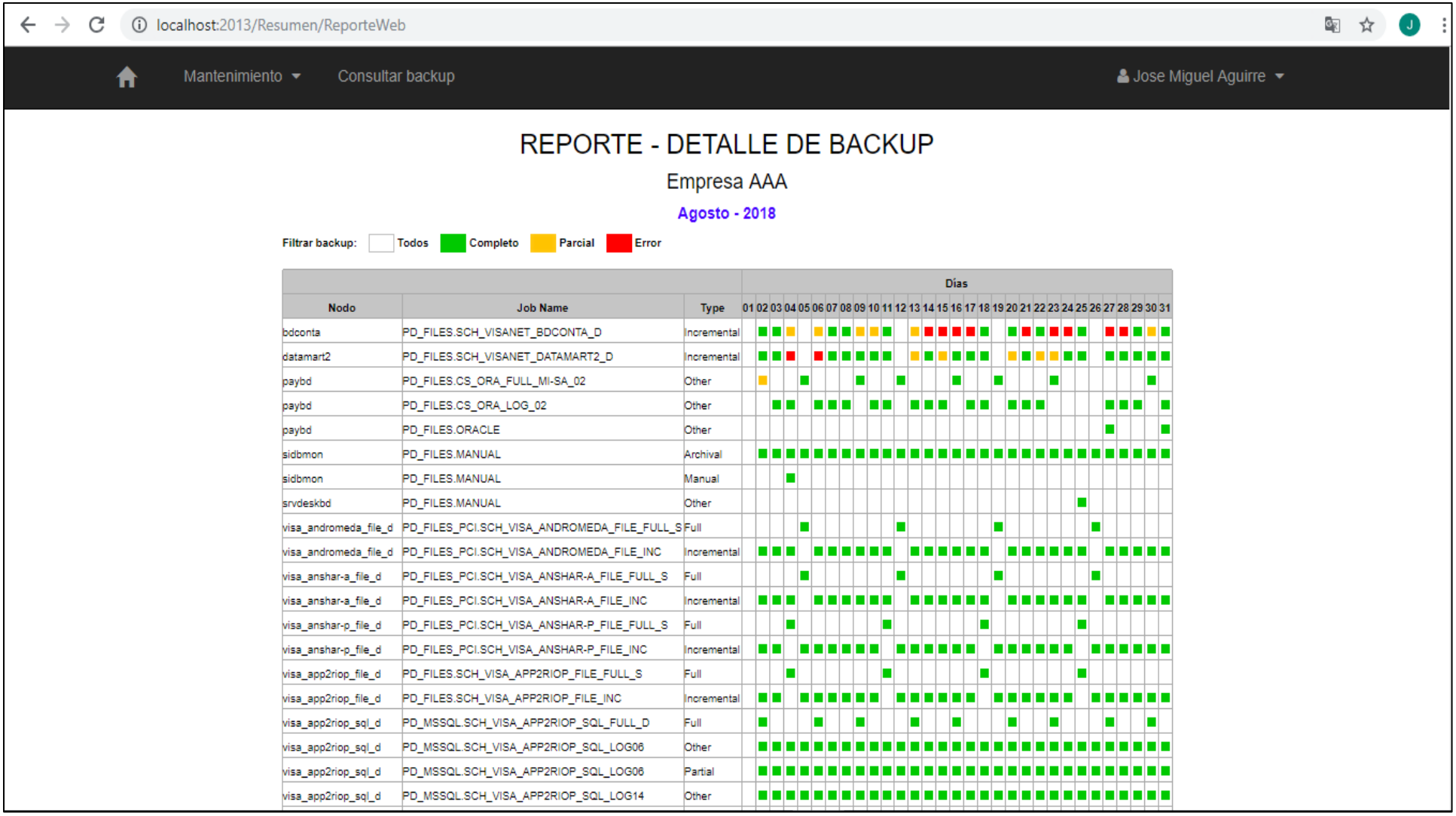
Pantalla Principal:

Generar reporte:



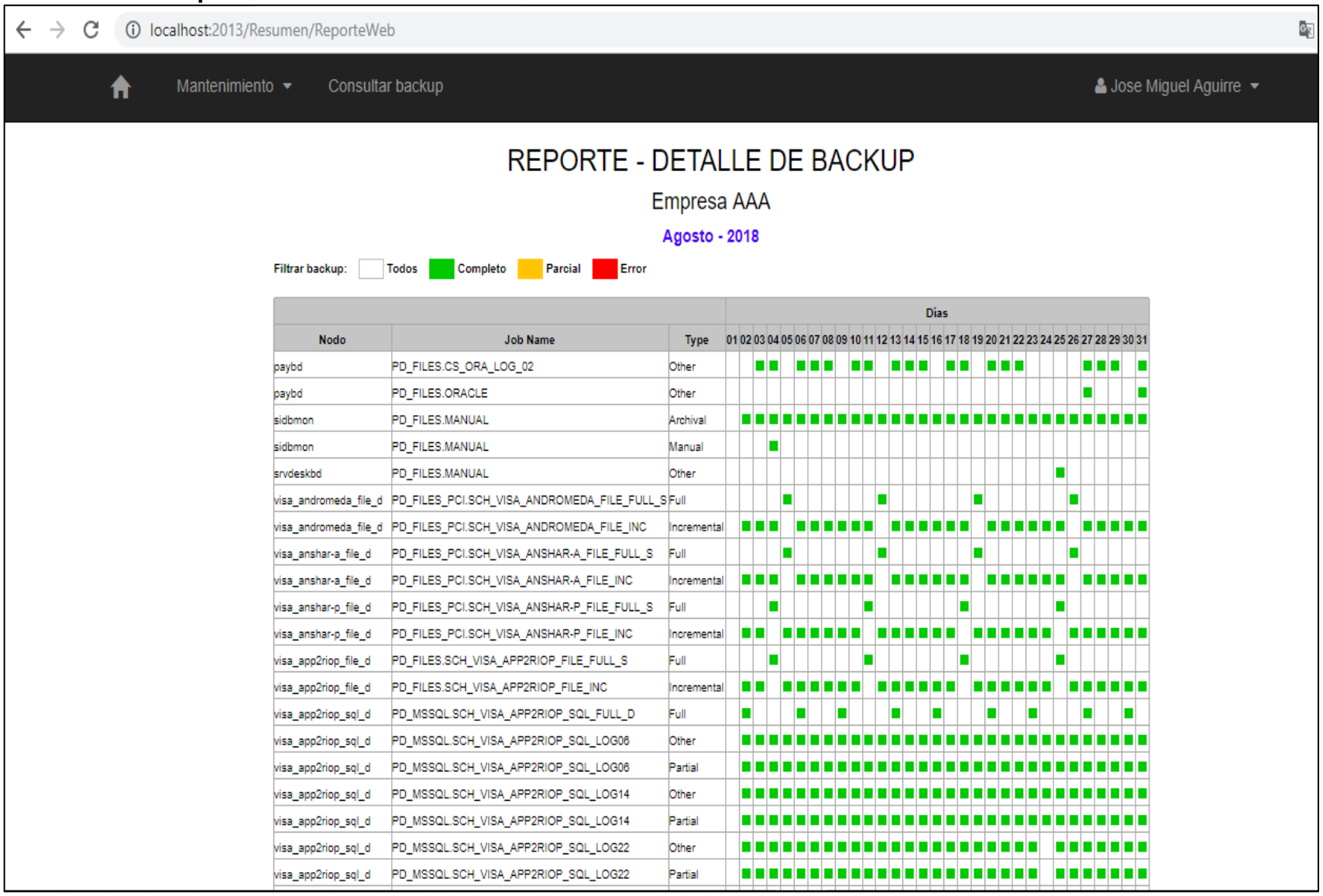
:

Reporte de backup mensuales

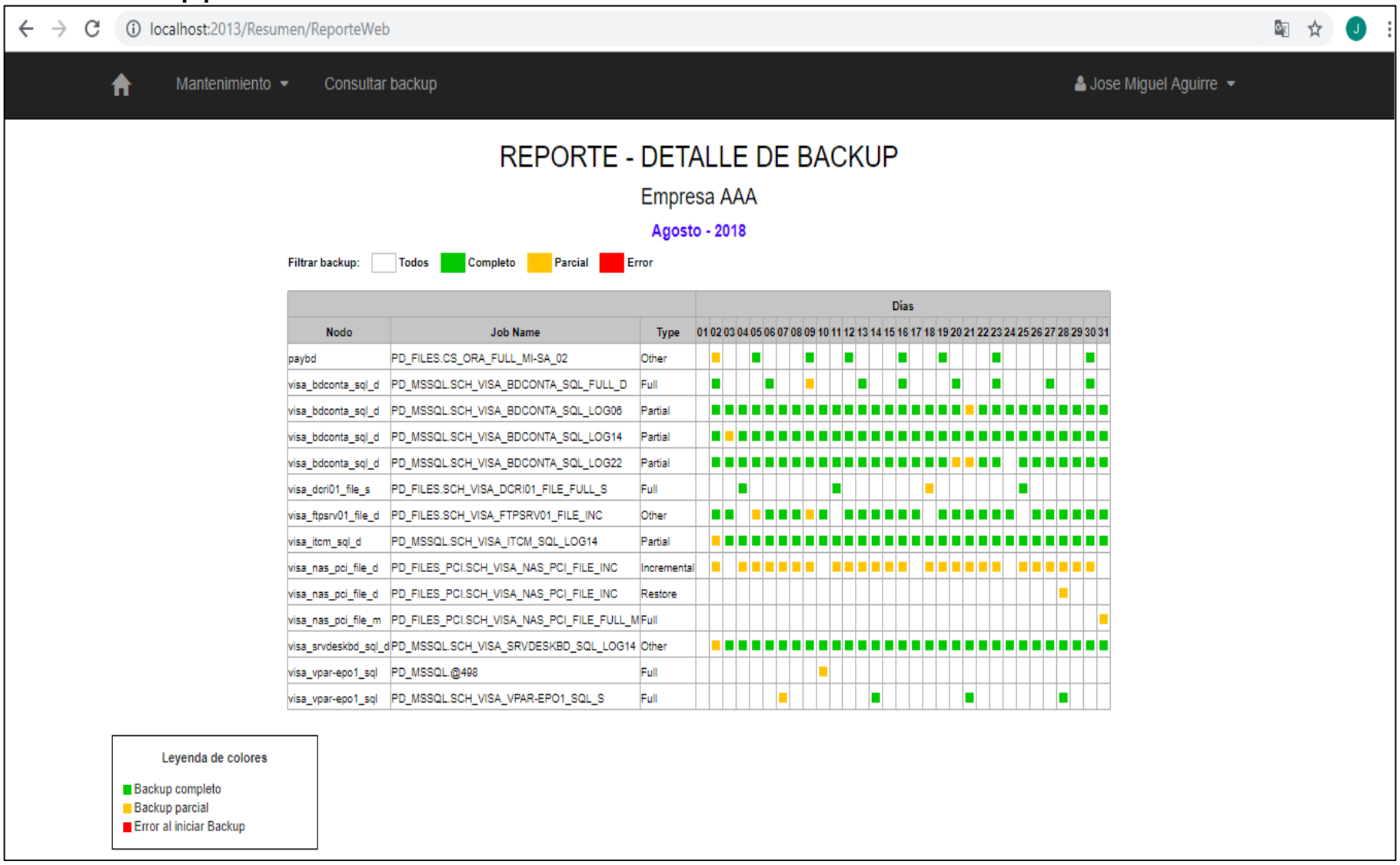


Nodo	Job Name	Type	Días
bdconta	PD_FILES.SCH_VISANET_BDCONTA_D	Incremental	
datamart2	PD_FILES.SCH_VISANET_DATAMART2_D	Incremental	
paybd	PD_FILES.CS_ORA_FULL_MI-SA_02	Other	
paybd	PD_FILES.CS_ORA_LOG_02	Other	
paybd	PD_FILES.ORACLE	Other	
sidbmon	PD_FILES.MANUAL	Archival	
sidbmon	PD_FILES.MANUAL	Manual	
srvdeskbd	PD_FILES.MANUAL	Other	
visa_andromeda_file_d	PD_FILES_PCI.SCH_VISA_ANDROMEDA_FILE_FULL_S	Full	
visa_andromeda_file_d	PD_FILES_PCI.SCH_VISA_ANDROMEDA_FILE_INC	Incremental	
visa_anshar-a_file_d	PD_FILES_PCI.SCH_VISA_ANSHAR-A_FILE_FULL_S	Full	
visa_anshar-a_file_d	PD_FILES_PCI.SCH_VISA_ANSHAR-A_FILE_INC	Incremental	
visa_anshar-p_file_d	PD_FILES_PCI.SCH_VISA_ANSHAR-P_FILE_FULL_S	Full	
visa_anshar-p_file_d	PD_FILES_PCI.SCH_VISA_ANSHAR-P_FILE_INC	Incremental	
visa_app2riop_file_d	PD_FILES.SCH_VISA_APP2RIOP_FILE_FULL_S	Full	
visa_app2riop_file_d	PD_FILES.SCH_VISA_APP2RIOP_FILE_INC	Incremental	
visa_app2riop_sql_d	PD_MSSQL.SCH_VISA_APP2RIOP_SQL_FULL_D	Full	
visa_app2riop_sql_d	PD_MSSQL.SCH_VISA_APP2RIOP_SQL_LOG06	Other	
visa_app2riop_sql_d	PD_MSSQL.SCH_VISA_APP2RIOP_SQL_LOG06	Partial	
visa_app2riop_sql_d	PD_MSSQL.SCH_VISA_APP2RIOP_SQL_LOG14	Other	

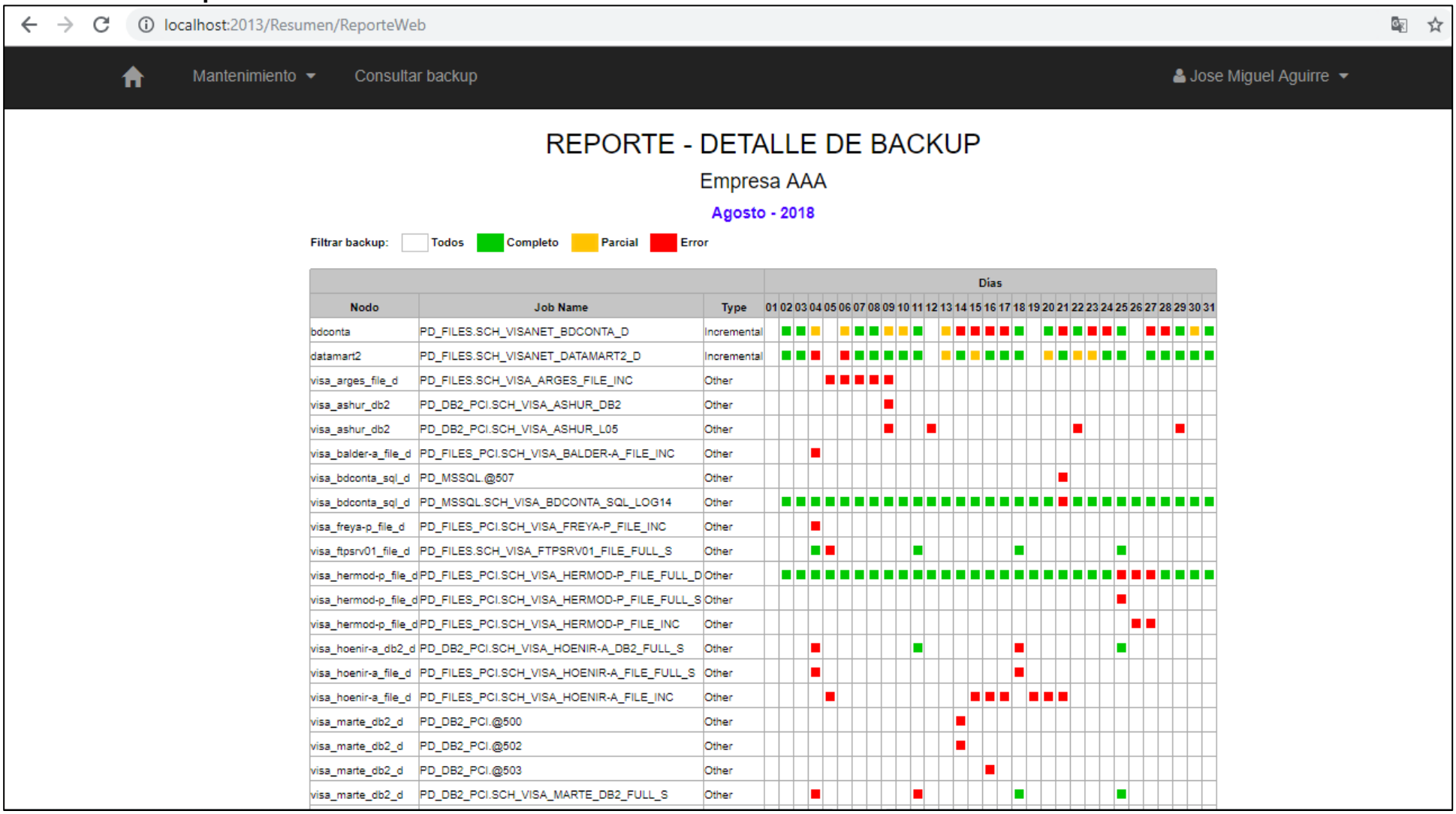
Filtrar solo backup satisfactorios:



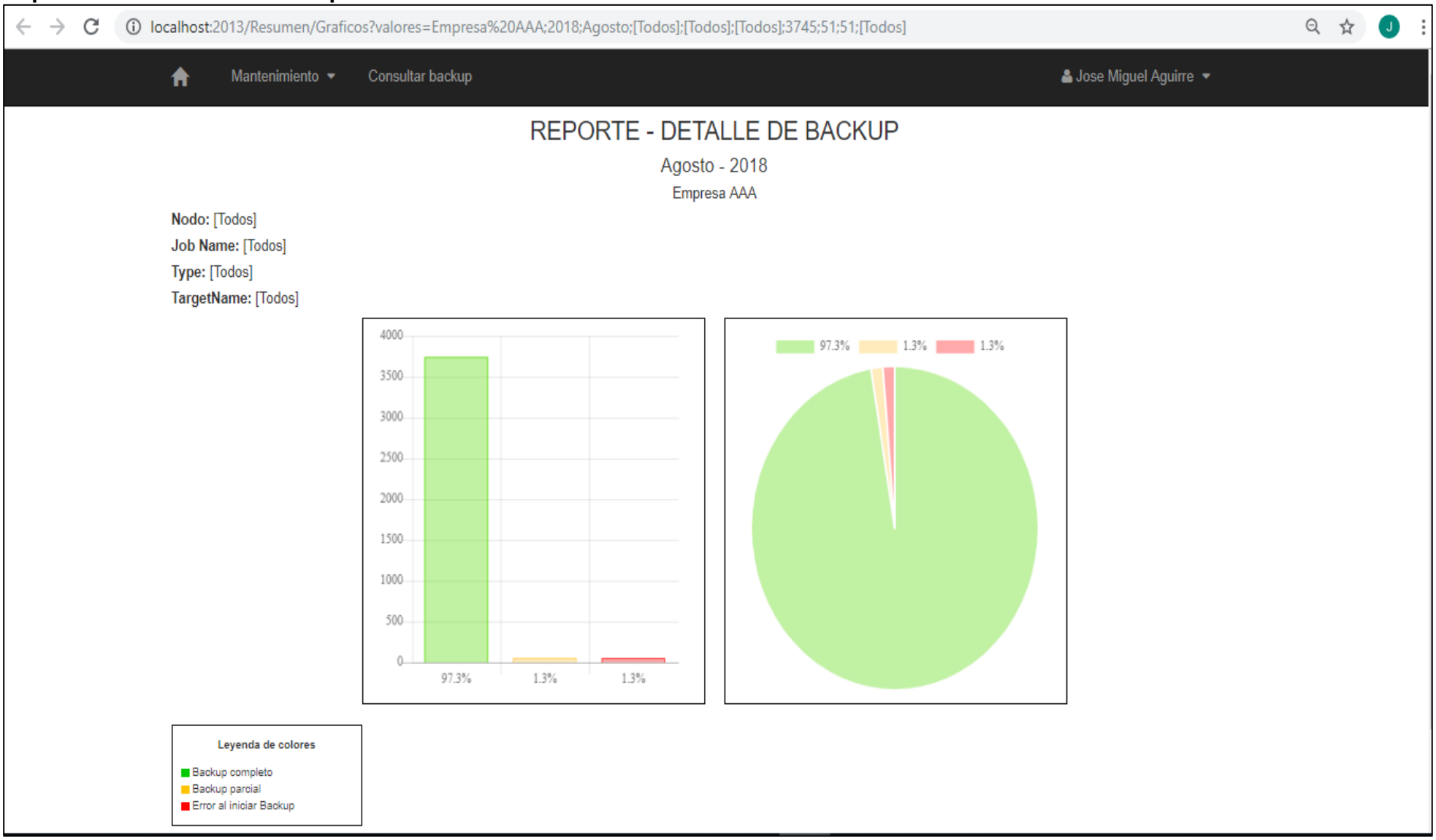
Filtra solo backup partial:



Filtrar solo backup Fallidos:



Reporte Estadístico de backup mensual:



UCV UNIVERSIDAD CÉSAR VALLEJO	ACTA DE APROBACIÓN DE ORIGINALIDAD DE TESIS	Código : F06-PP-PR-02.02 Versión : 09 Fecha : 23-03-2018 Página : 1 de 1

Yo, **FRANCISCO MANUEL HILARIO FALCON**, docente de la Facultad de Ingeniería y carrera Profesional de Ingeniería Sistemas de la Universidad César Vallejo campus Lima Este, revisor (a) de la tesis titulada:

"SISTEMA WEB PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ALINEADA A LA NORMA ISO/IEC 27001 EN LA EMPRESA DE SERVICIOS INFORMÁTICOS S.A.C – LA MOLINA", del estudiante **AGUIRRE VENTURA JOSE MIGUEL**, constato que la investigación tiene un índice de similitud de **29 %** verificable en el reporte de originalidad del programa Turnitin.

El/la suscrito(a) analizó dicho reporte y concluyó que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

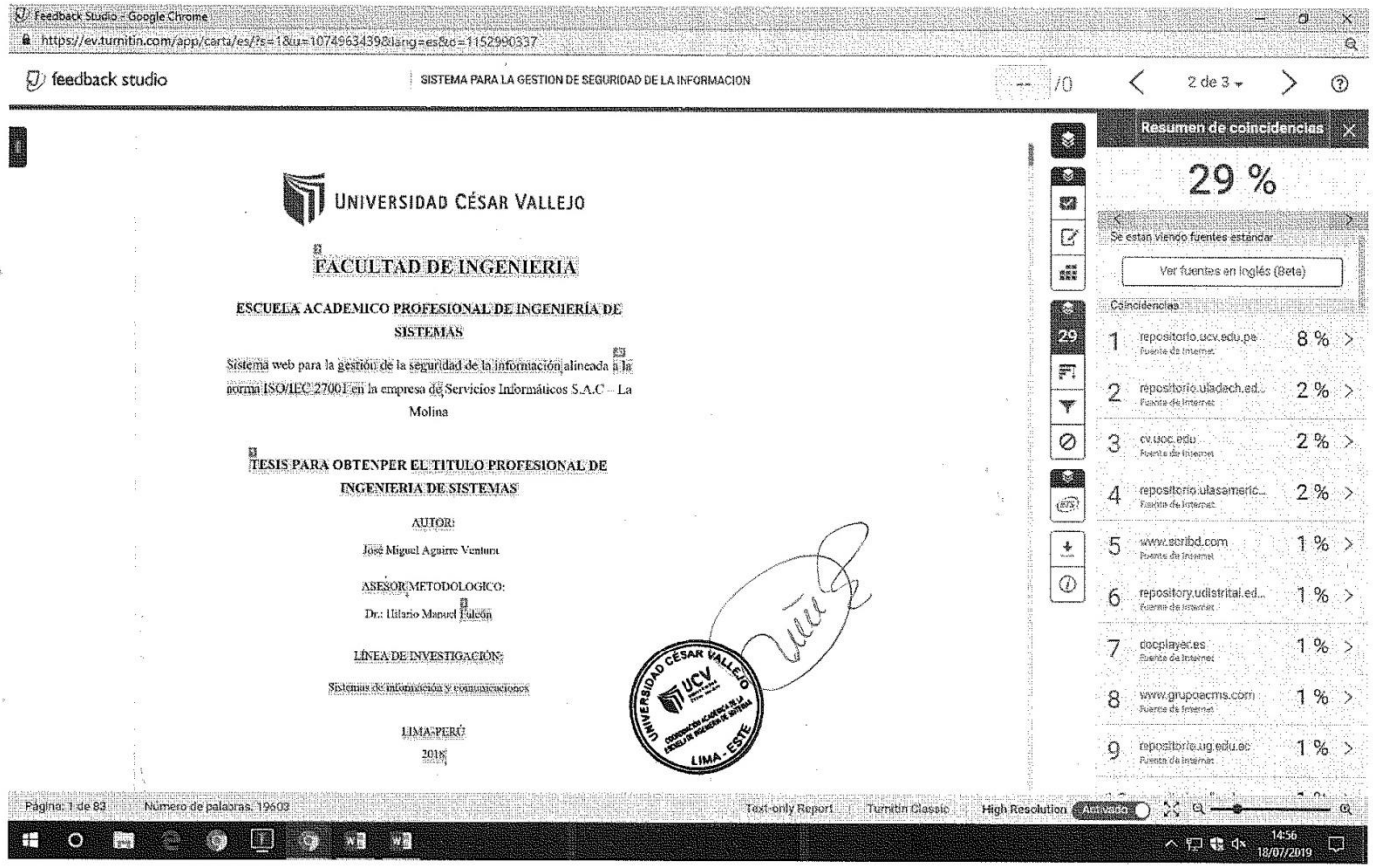
San Juan de Lurigancho, 19 de Diciembre del 2018

.....

FRANCISCO MANUEL HILARIO FALCON

DNI: 10132075

Elaboró	Dirección de Investigación	Revisó	Responsable del SGC	Aprobó	Vicerrectorado de Investigación


Feedback Studio - Google Chrome
https://ev.turnitin.com/app/carta/es/?s=1&u=1074963439&lang=es&o=1152990337
feedback studio
SISTEMA PARA LA GESTION DE SEGURIDAD DE LA INFORMACION
2 de 3
UNIVERSIDAD CÉSAR VALLEJO
FACULTAD DE INGENIERIA
ESCUELA ACADEMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS
Sistema web para la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de Servicios Informáticos S.A.C – La Molina
TESIS PARA OBTENPER EL TITULO PROFESIONAL DE INGENIERIA DE SISTEMAS
AUTOR:
José Miguel Aguirre Ventura
ASESOR METODOLOGICO:
Dr.: Hilario Manuel Falcón
LÍNEA DE INVESTIGACIÓN:
Sistemas de información y comunicaciones
LIMA-PERÚ
2018
UNIVERSIDAD CÉSAR VALLEJO
UCV
LIMA - ESTE
Resumen de coincidencias
29 %
Se están viendo fuentes estándar
Ver fuentes en Inglés (Beta)
Coincidencias
1 repositorio.ucv.edu.pe 8 %
2 repositorio.uladech.ed... 2 %
3 cv.uoc.edu 2 %
4 repositorio.ulasameric... 2 %
5 www.scribd.com 1 %
6 repository.udistrital.ed... 1 %
7 docplayer.es 1 %
8 www.grupoecms.com 1 %
9 repositorio.ug.edu.ec 1 %
Página: 1 de 83
Número de palabras: 19603
Text-only Report
Turnitin Classic
High Resolution
Activado
14:56
18/07/2019

UCV UNIVERSIDAD CÉSAR VALLEJO	AUTORIZACIÓN DE PUBLICACIÓN DE TESIS EN REPOSITORIO INSTITUCIONAL UCV	Código : F08-PP-PR-02.02 Versión : 09 Fecha : 23-03-2018 Página : 1 de 1

Yo **AGUITRRE VENTURA JOSE MIGUEL**, identificado con DNI N° **43061619**, egresado(a) de la Carrera Profesional de Ingeniería Sistemas de la Universidad César Vallejo, autorizo (X), no autorizo ( ) la divulgación y comunicación pública de mi trabajo de investigación titulado **"SISTEMA WEB PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ALINEADA A LA NORMA ISO/IEC 27001 EN LA EMPRESA DE SERVICIOS INFORMÁTICOS S.A.C – LA MOLINA".** en el Repositorio Institucional de la UCV (http://repositorio.ucv.edu.pe/), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art. 23 y Art. 33

Fundamentación en caso de no autorización:

.....
.....
.....
.....
.....
.....
.....
.....

.....
AGUITRRE VENTURA JOSE MIGUEL

DNI: **43061619**

Fecha: 19 de Diciembre del 2018

Elaboró	Dirección de Investigación	Revisó	Responsable del SGC	Aprobó	Dirección de Investigación

UNIVERSIDAD CÉSAR VALLEJO

AUTORIZACIÓN DE LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN

CONSTE POR EL PRESENTE EL VISTO BUENO QUE OTORGA EL ENCARGADO DE INVESTIGACIÓN DE

MARÌA ACUÑA MELÈNDEZ

A LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN QUE PRESENTA:

AGUIRRE VENTURA JOSÈ MIGUEL

INFORME TÍTULADO:

"SISTEMA WEB PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ALINEADA A LA NORMA ISO/IEC 27001 EN LA EMPRESA DE SERVICIOS INFORMÁTICOS S.A.C – LA MOLINA"

PARA OBTENER EL TÍTULO O GRADO DE:

INGENIERO DE SISTEMAS

SUSTENTADO EN FECHA: **19 DE DICIEMBRE DEL 2018**

NOTA O MENCIÓN: **(13) (TRECE).**

UNIVERSIDAD CÉSAR VALLEJO
UCV UNIVERSIDAD CÉSAR VALLEJO
COORDINACIÓN ACADÉMICA DE LA ESCUELA DE INGENIERÍA DE SISTEMAS
LIMA - ESTE

MARÌA ACUÑA MELÈNDEZ

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

07438294

CERTIFICADO DE INSCRIPCIÓN

N°00098037-19-RENIEC
El que suscribe certifica que a la fecha, obra en el Registro Único de Identificación de las Personas Naturales, la inscripción siguiente :

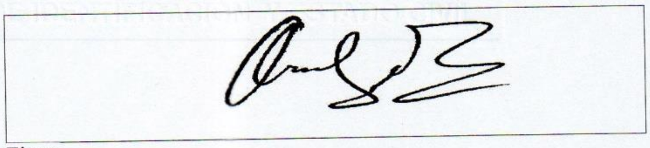
DNI Nº :43061619

TITULAR :AGUIRRE VENTURA, JOSE MIGUEL

Fecha Nacimiento	: 03/06/1985	Estatura	: 1.69mt.
Estado Civil	: DIVORCIADO	Grado Instrucción	: SECUNDARIA COMPLETA
Sexo	: MASCULINO	Doc. Sustento	: LIBRETA MILITAR Nº 8068501A1C
Fecha Inscripción	: 31/07/2003	Grupo Votación	: 232183
Lugar Inscripción	: LIMA/LIMA/SAN JUAN DE LURIGANCHO		
Dirección	: JR.LOS AZULEJOS 458 URB.SAN CARLOS**		
Fecha Cancelación	: **	Motivo Cancelación	: **
Glosa Informativa	: **		

IMÁGENES


Foto


Firma

De lo que doy fe, en SAN JUAN DE LURIGANCHO a los 21 dias del mes de Junio del 2019
Esta certificación caduca e **21 de Julio del 2019**
(Cualquier enmendadura o adición invalida el presente documento)

Solicitante:
Sr(es).AGUIRRE VENTURA ,JOSE MIGUEL

Pag.: 1/

...Final

Tot.Reg.

(20038600098037CI12920010285120038620190621)

RENIEC

00098037

LINDA KARINA HUAMAN CULQUICON
DNI 10577013
Certificador
Jefatura Regional Lima
RENIEC